

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-123084
(P2000-123084A)

(43) 公開日 平成12年4月28日 (2000. 4. 28)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 17/60		G 0 6 F 15/21	Z 5 B 0 4 9
13/00	3 5 1	13/00	3 5 1 G 5 B 0 8 9
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 B 5 J 1 0 4
			6 6 0 E 5 K 0 2 5
5/00		5/00	5 K 0 3 0
審査請求 未請求 請求項の数 7 O L (全 69 頁) 最終頁に続く			

(21) 出願番号 特願平10-293830

(22) 出願日 平成10年10月15日 (1998. 10. 15)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川 6 丁目 7 番35号

(72) 発明者 松山 科子

東京都品川区北品川 6 丁目 7 番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

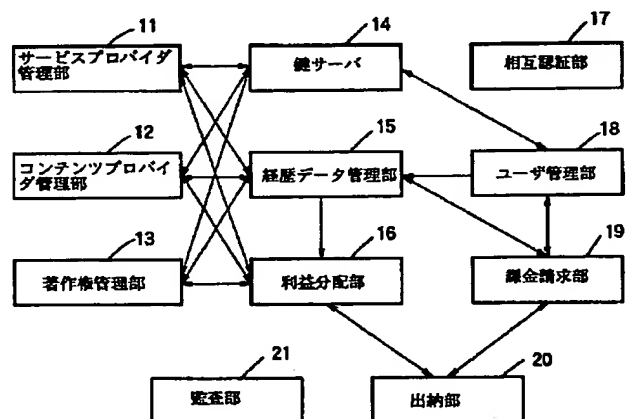
最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理方法、および提供媒体

(57) 【要約】

【課題】 精算処理および利益の算出の処理を効率良く出来るようにする。

【解決手段】 利益分配部 16 は、情報を特定するデータおよび情報の利用に対する情報提供者の支払い金額を示すデータを記憶し、その記憶するデータを基に、情報提供者毎の支払い金額の合計を算出する。出納部 20 は、利益分配部 16 が算出した情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する。



EMD サービスセンタ 1

【特許請求の範囲】

【請求項 1】 情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理装置において、前記情報を特定するデータおよび前記情報の利用に対する前記情報提供者への支払い金額を示すデータを記憶する記憶手段と、

前記記憶手段が記憶するデータを基に、前記情報提供者毎への支払い金額の合計を算出する算出手段と、
前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示手段とを備えることを特徴とする情報処理装置。

【請求項 2】 前記算出手段は、前記情報提供者間の支払金額の合計をさらに算出することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記記憶手段は、前記情報の著作権を徴収する団体への支払い金額に関する情報をさらに記憶し、

前記算出手段は、前記団体への支払い金額の合計をさらに算出し、

前記決済指示手段は、前記決済機関に対し前記団体の決済をさらに指示することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記記憶手段は、情報の利用料金の割引のデータをさらに記憶することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記決済指示手段は、前記情報提供者毎の決済機関に関する情報を記憶することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理方法において、前記情報を特定するデータおよび前記情報の利用に対する前記情報提供者への支払い金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供者毎への支払い金額の合計を算出する算出ステップと、

前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示ステップとを含むことを特徴とする情報処理方法。

【請求項 7】 情報提供者に代わり、前記情報提供者が提供する情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理装置に、前記情報を特定するデータおよび前記情報の利用に対する前記情報提供者への支払い金額を示すデータを記憶する記憶ステップと、

前記記憶ステップで記憶するデータを基に、前記情報提供者毎への支払い金額の合計を算出する算出ステップと、

前記情報提供者毎の利益を基に、決済機関に対し前記情報提供者毎の決済を指示する決済指示ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理装置、情報処理方法、および提供媒体に関し、特に、情報提供者に代わり、情報の利用者から利用料金を徴収し、情報提供者に利益を分配する情報処理装置、情報処理方法、および提供媒体に関する。

【0002】

【従来の技術】 音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、再生するシステムがある。情報提供者は、複数の情報提供者に、情報を送信し、サービスを提供することができる。

【0003】

【発明が解決しようとする課題】 情報提供者は、複数のユーザ毎に、契約し、利用料金を精算しなければならず、また、精算処理および利益の算出処理を行わなければならない、無駄が多い。

【0004】 本発明はこのような状況に鑑みてなされたものであり、精算処理および利益の算出の処理を効率良く出来るようにすることを目的とする。

【0005】

【課題を解決するための手段】 請求項 1 に記載の情報処理装置は、情報を特定するデータおよび情報の利用に対する情報提供者への支払い金額を示すデータを記憶する記憶手段と、記憶手段が記憶するデータを基に、情報提供者毎への支払い金額の合計を算出する算出手段と、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する決済指示手段とを備えることを特徴とする。

【0006】 請求項 6 に記載の情報処理方法は、情報を特定するデータおよび情報の利用に対する情報提供者への支払い金額を示すデータを記憶する記憶ステップと、記憶ステップで記憶するデータを基に、情報提供者毎への支払い金額の合計を算出する算出ステップと、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する決済指示ステップとを含むことを特徴とする。

【0007】 請求項 7 に記載の提供媒体は、情報処理装置に、情報を特定するデータおよび情報の利用に対する情報提供者への支払い金額を示すデータを記憶する記憶ステップと、記憶ステップで記憶するデータを基に、情報提供者毎への支払い金額の合計を算出する算出ステップと、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する決済指示ステップとを含む処理を実行させるコンピュータが読み取り可能な

プログラムを提供することを特徴とする。

【0008】請求項1に記載の情報処理装置、請求項6に記載の情報処理方法、および請求項7に記載の提供媒体においては、情報を特定するデータおよび情報の利用に対する情報提供者への支払い金額を示すデータを記憶し、記憶するデータを基に、情報提供者毎への支払い金額の合計を算出し、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する。

【0009】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0010】すなわち、請求項1に記載の情報処理装置は、情報を特定するデータおよび情報の利用に対する情報提供者への支払い金額を示すデータを記憶する記憶手段（例えば、図2の利益分配部16）と、記憶手段が記憶するデータを基に、情報提供者毎への支払い金額の合計を算出する算出手段（例えば、図2の利益分配部16）と、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示する決済指示手段（例えば、図2の出納部20）とを備えることを特徴とする。

【0011】図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。EMDサービスセンタ1は、コンテンツプロバイダ2、ユーザホームネットワーク5等に配送用鍵Kdを送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等を受信し、利用料金を精算し、コンテンツプロバイダ2およびサービスプロバイダ3への利益分配の処理を行う。

【0012】コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するためのウォーターマーク（電子透かし）をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、所定の情報を付加して、サービスプロバイダ3に送信する。

【0013】サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格を付して、ユーザホームネットワーク5に送信する。

【0014】ユーザホームネットワーク5は、サービスプロバイダ3から価格を付して送付されたコンテンツを入手し、コンテンツを復号、再生して利用するとともに

課金処理を実行する。課金処理により得られた課金情報は、ユーザホームネットワーク5が配送用鍵KdをEMDサービスセンタ1から入手する際、EMDサービスセンタ1に送信される。

【0015】図2は、EMDサービスセンタ1の機能の構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給するとともに、コンテンツプロバイダ2から供給されるコンテンツに付される情報（取扱方針）が暗号化されている場合、サービスプロバイダ3に配送用鍵Kdを送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信するとともに、利益分配の情報を供給する。著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。鍵サーバ14は、配送用鍵Kdを記憶しており、コンテンツプロバイダ管理部12、またはユーザ管理部18等を介して、配送用鍵Kdをコンテンツプロバイダ2、またはユーザホームネットワーク5等に供給する。ユーザ管理部18は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報である課金情報、そのコンテンツに対応する価格情報、およびそのコンテンツに対応する取扱方針を入力し、経歴データ管理部15に記憶させる。

【0016】EMDサービスセンタ1からコンテンツプロバイダ2およびユーザホームネットワーク5を構成するレシーバ51（図10で後述する）への、配送用鍵Kdの定期的な送信の例について、図3乃至図6を参照に説明する。図3は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

【0017】図3の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である“aaaaaaaa”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）であり、所定のビット数の乱数である“bbbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコ

ンテンツを暗号化するコンテンツ鍵Kc oは、バージョン2である配送用鍵Kdで暗号化されている)である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

【0018】コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0019】また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0020】1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0021】1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図4で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K

dをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

【0022】1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

10 【0023】1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdおよびバージョン2である配送用鍵Kdをそのまま記憶する。

【0024】1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0025】1998年4月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン4乃至バージョン6である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kd、バージョン2である配送用鍵Kd、およびバージョン3である配送用鍵Kdをそのまま記憶する。

【0026】1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵Kdが、

EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0027】このように、あらかじめ先の月の配送用鍵Kdを配布しておくことで、仮にユーザーが1、2ヶ月まったくセンターにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センターにアクセスして鍵を受信することができる。

【0028】利益分配部16は、経歴データ管理部15から供給された、課金情報、価格情報、および取扱方針に基づき、EMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益を算出する。相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の所定の機器と後述する相互認証を実行する。

【0029】ユーザ管理部18は、ユーザ登録データベースを有し、ユーザホームネットワーク5の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒絶する等の処理を実行する。ユーザホームネットワーク5がEMDサービスセンタ1と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部18は、登録が可能か否かの判定の処理の結果に対応して、決済をする機器を指定し、さらに、コンテンツの利用条件を規定した登録リストをユーザホームネットワーク5の所定の機器に送信する。

【0030】図7に示すユーザ登録データベースの例は、ユーザホームネットワーク5の機器の機器固有の64ビットからなるID (Identification Data) を記録し、そのIDに対応して（すなわち、そのIDを有する機器毎に）、決済処理が可能か否か、登録が可能か否か、EMDサービスセンタ1と接続が可能か否か等の情報を記録する。ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはサービスプロバイダ3などから供給される料金の未払い、不正処理等の情報を基に、所定の時間間隔で更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を拒否し、登録を拒否された機器は、以後、このシステムのコンテンツを利用できない。

【0031】ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの再生またはコピーなどの利用が可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、EMDサービスセンタ1に、ユーザホームネットワーク5のEMDサービスセンタ1に登録されている全ての機器の、課金情報、価格情報、および取扱方針を出力する。ユーザ登録データベースに記録されたEMDサービスセンタ1と接続が可能か否かの情報は、その機器

が、EMDサービスセンタ1と接続が可能であるか否かを示し、接続ができないと記録された機器は、ユーザホームネットワーク5の他の機器を介して、EMDサービスセンタ1に、課金情報等を出力する。

【0032】また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、価格情報、および取扱方針が供給され、その情報を経歴データ管理部15に出力し、さらに、所定の処理（タイミング）で、ユーザホームネットワーク5の機器に、配送用鍵Kdを供給する。

【0033】課金請求部19は、経歴データ管理部15から供給された、課金情報、価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性（すなわち、不正をしていないか）を監査する。

【0034】図8は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部32に供給する。ウォータマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォータマークを付加し、圧縮部33に供給する。圧縮部33は、ウォータマーク付加部32から供給されたコンテンツを、ATRAC2 (Adaptive Transform Acoustic Coding 2) (商標) 等の方式で圧縮し、暗号化部34に供給する。暗号化部34は、圧縮部33で圧縮されたコンテンツを、乱数発生部35から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Kcoと称する）として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

【0035】乱数発生部35は、コンテンツ鍵Kcoとなる所定のビット数の乱数を暗号化部34および暗号化部36に供給する。暗号化部36は、コンテンツ鍵KcoをEMDサービスセンタ1から供給された配送用鍵Kdを使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

【0036】DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0037】まず、平文の64ビットは、上位32ビット

トの H_0 、および下位 3 2 ビットの L_0 に分割される。鍵処理部から供給された 4 8 ビットの拡大鍵 K_1 、および下位 3 2 ビットの L_0 を入力とし、下位 3 2 ビットの L_0 を搅拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 3 2 ビットの H_0 と、F 関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【0 0 3 8】上位 3 2 ビットの H_0 および下位 3 2 ビットの L_0 を基に、以上の処理を 1 6 回繰り返す、得られた上位 3 2 ビットの H_1 、および下位 3 2 ビットの L_1 が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0 0 3 9】ポリシー記憶部 3 7 は、コンテンツの取扱方針（ポリシー）を記憶し、暗号化されるコンテンツに対応して、取扱方針をセキュアコンテナ作成部 3 8 に出力する。セキュアコンテナ作成部 3 8 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、取扱方針、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 K_{co} 、および取扱方針のハッシュ値をとり作成された署名、さらにコンテンツプロバイダ 2 の公開鍵 K_{pcp} を含む証明書から構成されるコンテンツプロバイダセキュアコンテナを作成し、サービスプロバイダ 3 に供給する。相互認証部 3 9 は、EMD サービスセンタ 1 から配送用鍵 K_d の供給を受けるのに先立ち、EMD サービスセンタ 1 と相互認証し、また、サービスプロバイダ 3 へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ 3 と相互認証する。

【0 0 4 0】署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0 0 4 1】ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化するとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0 0 4 2】署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと

判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4、MD5、SHA-1などが用いられる。

【0 0 4 3】次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0 0 4 4】公開鍵暗号の中で代表的な RSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2 つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3 以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1 のみである）。

【0 0 4 5】次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \pmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p 、 q 、および d が、秘密鍵とされる。

【0 0 4 6】暗号文 C は、明文 M から、式 (1) の処理で算出される。

$$C=M^e \pmod n \quad (1)$$

【0 0 4 7】暗号文 C は、式 (2) の処理で明文 M に、復号される。

$$M=C^d \pmod n \quad (2)$$

【0 0 4 8】証明は省略するが、RSA 暗号で明文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおりており、式 (3) が成立するからである。

$$M=C^d=(M^e)^d=M^{ed} \pmod n \quad (3)$$

【0 0 4 9】秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA 暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0 0 5 0】また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2=x^3+ax+tb$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、明文 M から、公開鍵で式 (4) および式 (5) の処理で算出される。

$C1 = M + rnB$ (4)

$C2 = rB$ (5)

【0051】暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

$M = C1 - nC2$ (6)

【0052】復号できるのは、秘密鍵nを有するものである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0053】図9は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、暗号化されているコンテンツを記憶し、セキュアコンテナ作成部44に供給する。値付け部42は、コンテンツに対応した取扱方針を基に、価格情報を作成し、セキュアコンテナ作成部44に供給する。ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツの取扱方針を記憶し、セキュアコンテナ作成部44に供給する。相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証し、また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証する。また、コンテンツプロバイダ2が取扱方針を配送用鍵Kdで暗号化して供給する場合、相互認証部45は、EMDサービスセンタ1から配送用鍵Kdの供給を受け付けるのに先立ち、EMDサービスセンタ1と相互認証する。

【0054】図10は、ユーザホームネットワーク5の構成を示すブロック図である。レシーバ51は、ネットワーク4を介して、サービスプロバイダ3からコンテンツを含んだサービスプロバイダセキュアコンテナを受信し、コンテンツを復号および伸張し、再生する。

【0055】通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。SAM(Secure Application Module)62は、サービスプロバイダ3、またはEMDサービスセンタ1と相互認証し、コンテンツの暗号を復号し、またはコンテンツを暗号化し、さらに配送用鍵Kd等を記憶する。伸張部63は、コンテンツの暗号を復号し、ATRAC2方式で伸張し、さらに所定のウォータマークをコンテンツに挿入する。IC(Integrated Circuit)カードインターフェース64は、SAM62からの信号を所定の形式に変更し、レシーバ51に装着されたICカード55に出力し、また、ICカード55からの信号を所定の形式に変更し、SAM62に出力する。

【0056】サービスプロバイダ3、またはEMDサービスセンタ1と相互認証し、課金処理を実行し、コンテンツ鍵Kcoを復号および暗号化し、さらに使用許諾条件情報等の所定のデータを記憶するSAM62は、相互認証

モジュール71、課金モジュール72、記憶モジュール73、および復号/暗号化モジュール74から構成される。このSAM62は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性(耐タンパー性)を有する。

【0057】相互認証モジュール71は、サービスプロバイダ3、またはEMDサービスセンタ1との相互認証を実行し、必要に応じて、一時鍵Ktemp(セッション鍵)を復号/暗号化モジュール74に供給する。課金処理モジュール72は、サービスプロバイダ3から受信したサービスプロバイダセキュアコンテナに含まれる取扱方針および価格情報(並びに、場合によっては、取扱制御情報)から、使用許諾条件情報および課金情報を生成し、記憶モジュール73またはHDD(Hard Disk Drive)52に出力する。記憶モジュール73は、課金処理モジュール72または復号/暗号化モジュール74から供給された課金情報、および配送用鍵Kd等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送用鍵Kd等のデータを供給する。

【0058】復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、所定の桁数の乱数を発生し、保存用鍵Ksaveとして暗号化ユニット93および記憶モジュール73に出力する。ただし、一度生成して保持している場合、生成の必要はない。暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、保存用鍵Ksaveで暗号化し、HDD52に出力する。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部63に送信するとき、コンテンツ鍵Kcoを一時鍵Ktempで暗号化する。

【0059】コンテンツを復号し、伸張し、所定のウォータマークを付加する伸張部63は、相互認証モジュール75、復号モジュール76、復号モジュール77、伸張モジュール78、およびウォータマーク付加モジュール79から構成される。相互認証モジュール75は、SAM62と相互認証し、一時鍵Ktempを復号モジュール76に出力する。復号モジュール76は、記憶モジュール73から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール77に出力する。復号モジュール77は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール78に出力する。伸張モジュール78は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォータマーク付加モジュール79に出力する。ウォータマーク付加モジュール79は、コンテンツにレシーバ51を特定する所定のウォータマークを

挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0060】HDD52は、サービスプロバイダ3から供給されたコンテンツを記録する。装着された光ディスク（図示せず）にサービスプロバイダ3から供給されたコンテンツを記録し、再生するレコーダ53は、記録再生部65、SAM66、および伸張部67から構成される。記録再生部65は、光ディスクが装着され、その光ディスクにコンテンツを記録し、再生する。SAM66は、SAM62と同じ機能を有し、その説明は省略する。伸張部67は、伸張部63と同じ機能を有し、その説明は省略する。MD(Mini Disk:商標)ドライブ54は、装着された図示せぬMDにサービスプロバイダ3から供給されたコンテンツを記録し、再生する。

【0061】ICカード55は、レシーバ51に装着され、記憶モジュール73に記憶された配送用鍵Kdおよび機器のIDなどの所定のデータを記憶する。例えば、新たなレシーバ51を購入し、今まで使用していたレシーバ51と入れ替えて使用する場合、まず、ユーザは、ICカード55に、今まで使用していたレシーバ51の記憶モジュール73に記憶されていた配送用鍵Kdなどの所定のデータを記憶させる。次に、ユーザは、そのICカード55を新たなレシーバ51に装着し、そのレシーバ51を操作して、EMDサービスセンタ1のユーザ管理部18にその新たなレシーバ51を登録する。EMDサービスセンタ1のユーザ管理部18は、ICカード55に記憶されていたデータ（今まで使用していたレシーバ51のIDなど）を基に、ユーザ管理部18が保持しているデータベースから、ユーザの氏名、使用料の払い込みを使用するクレジットカードの番号などのデータを検索し、そのデータを基に、登録の処理を実行するので、ユーザは、面倒なデータを入力する必要がない。ICカード55は、相互認証モジュール80および記憶モジュール81で構成される。相互認証モジュール80は、SAM62と相互認証する。記憶モジュール81は、ICカードインターフェース64を介して、SAM62から供給されたデータを記憶し、記憶したデータをSAM62に出力する。

【0062】図11は、ユーザホームネットワーク5の他の構成例を示すブロック図である。この構成のレシーバ51およびレコーダ53は、図10に示した伸張部63および伸張部67を省略した構成を有する。その代わり、レコーダ53に接続されているデコーダ56が、伸張部63または伸張部67と同じ機能を有する。その他の構成は、図10における場合と同様である。

【0063】コンテンツを復号し、伸張し、ウォーターマークを付加するデコーダ56は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62またはSAM66と相互認証し、一時鍵Kt

empを復号モジュール102に出力する。復号モジュール102は、SAM62から出力され、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRAC2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。ウォーターマーク付加モジュール105は、コンテンツにデコーダ56を特定する所定のウォーターマークを挿入し、レコーダ53に出力したり、図示せぬスピーカに出力し、音楽を再生する。

【0064】図12は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、および署名をコンテンツプロバイダセキュアコンテナ（その詳細は図13を参照して後述する）に格納し、さらにコンテンツプロバイダセキュアコンテナにコンテンツプロバイダ2の証明書（その詳細は図14を参照して後述する）を付して、サービスプロバイダ3に送信する。コンテンツプロバイダ2はまた、取扱方針、および署名にコンテンツプロバイダ2の証明書を付して、EMDサービスセンタ1に送信する。

【0065】サービスプロバイダ3は、受信したコンテンツプロバイダセキュアコンテナに含まれる取扱方針を基に価格情報を生成し、暗号化されたコンテンツ、暗号化されたコンテンツ鍵Kco、取扱方針、価格情報、および署名をサービスプロバイダセキュアコンテナ（その詳細は図15を参照して後述する）に格納し、さらにサービスプロバイダセキュアコンテナにサービスプロバイダ3の証明書（その詳細は図16を参照して後述する）を付して、ユーザホームネットワーク5に送信する。サービスプロバイダ3はまた、価格情報、および署名にサービスプロバイダ3の証明書を付して、EMDサービスセンタ1に送信する。

【0066】ユーザホームネットワーク5は、受信したサービスプロバイダセキュアコンテナに含まれる取扱方針から使用許諾情報を生成し、使用許諾情報に沿って、コンテンツを利用する。ユーザホームネットワーク5において、コンテンツ鍵Kcoが復号されると、課金情報が生成される。課金情報は、所定のタイミングで、暗号化され、取扱方針と共に署名が付され、EMDサービスセンタ1に送信される。

【0067】EMDサービスセンタ1は、課金情報および取扱方針を基に使用料金を算出し、またEMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3それぞれの利益を算出する。EMDサービスセン

タ 1 は、さらに、コンテンツプロバイダ 2 から受信した取扱方針、サービスプロバイダ 3 から受信した価格情報、並びにユーザホームネットワーク 5 から受信した課金情報および取扱方針を比較し、サービスプロバイダ 3 またはユーザホームネットワーク 5 で取扱方針の改竄または不正な価格の付加等の不正がなかったか否かを監査する。

【0068】図 13 は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o、取扱方針、および署名を含む。署名は、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o、および取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ 2 の秘密鍵 K s c p で暗号化したデータである。

【0069】図 14 は、コンテンツプロバイダ 2 の証明書 を説明する図である。コンテンツプロバイダ 2 の証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダの公開鍵 K p c p、並びに署名を含む。署名は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、コンテンツプロバイダ 2 の名前、並びにコンテンツプロバイダの公開鍵 K p c p にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K s c a で暗号化したデータである。

【0070】図 15 は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o、取扱方針、価格情報、および署名を含む。署名は、コンテンツ鍵 K c o で暗号化されたコンテンツ、配送用鍵 K d で暗号化されたコンテンツ鍵 K c o、取扱方針、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ 3 の秘密鍵 K s s p で暗号化したデータである。

【0071】図 16 は、サービスプロバイダ 3 の証明書を説明する図である。サービスプロバイダ 3 の証明書は、証明書のバージョン番号、認証局がサービスプロバイダ 3 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 の名前、サービスプロバイダの公開鍵 K p s p、並びに署名を含む。署名は、証明書のバージョン番号、認証局がサービスプロバイダ 3 に対し割り付ける証明書の通し番号、署名に用い

たアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 の名前、サービスプロバイダの公開鍵 K p s p にハッシュ関数を適用して生成されたハッシュ値を、認証局の秘密鍵 K s c a で暗号化したデータである。

【0072】図 17 は、取扱方針、価格情報、および使用許諾条件情報を示す図である。コンテンツプロバイダ 2 が有する取扱方針 (図 17 (A)) は、コンテンツ毎に用意され、ユーザホームネットワーク 5 が利用可能な利用内容を示す。例えば、図 17 (A) の取り扱い方針は、ユーザホームネットワーク 5 がそのコンテンツを再生およびマルチコピーすることは許可するが、シングルコピーは許可しないことを示す。

【0073】図 18 は、シングルコピーおよびマルチコピーを説明する図である。マルチコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、複数のコピーを作成することを行う。ただし、図 18 (A) に示すように、コピーを更にコピーすることはできない (許されない)。シングルコピーは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合において、そのコンテンツから、ただ 1 つのコピーを作成することを行う。シングルコピーの場合も、図 18 (B) に示すように、コピーを更にコピーすることはできない (許されない)。

【0074】サービスプロバイダ 3 は、図 17 (B) に示すように、コンテンツプロバイダ 2 からの取扱方針 (図 17 (A)) に価格情報を加える。例えば、図 17 (B) の価格情報は、そのコンテンツを再生して利用するときの料金が 150 円で、マルチコピーして利用するときの利用料金が 80 円であることを示す。図 17 には、例示しないが、シングルコピーの価格情報は、コピーの 1 回当たりの使用料金を表し、例えば、3 回のコピーの利用では、シングルコピーの使用料金の 3 倍の料金を支払う。マルチコピーまたはシングルコピーが許可されるコンテンツは、使用許諾条件情報においてコピー許可が与えられているコンテンツに対し、その使用許諾条件を購入した場合における、そのコンテンツに限られる。

【0075】ユーザホームネットワーク 5 は、サービスプロバイダ 3 から供給される取扱方針が示すコンテンツの利用可能な利用内容 (図 17 (B)) から、ユーザが選択した、利用内容を示す使用許諾条件情報 (図 17 (C)) を記憶する。例えば、図 17 (C) の使用許諾条件情報は、そのコンテンツを再生して使用することができ、シングルコピーおよびマルチコピーができないことを示す。

【0076】図 19 は、図 17 の例と比較してコンテンツプロバイダ 2 が取扱方針に利益分配の情報を加え、サ

10

20

30

40

50

ービスプロバイダ3が価格情報に利益分配の情報を加える場合の、取扱方針および価格情報を説明する図である。図17に示す例に対して、図19の例では、コンテンツプロバイダ2の利益が、コンテンツを再生して利用するとき70円で、マルチコピーして利用するとき40円であることを示す情報が、追加されている(図19

(A))。更に、利益分配情報として、サービスプロバイダ3の利益が、コンテンツを再生して利用するとき60円で、マルチコピーして利用するとき30円であることが、追加されている(図19(B))。価格は、図17(A)における場合と同様に、再生が150円、マルチコピーが40円とされている。価格(例えば150円)からコンテンツプロバイダ2の利益(例えば70円)およびサービスプロバイダ3の利益(例えば60円)を差し引いた金額(例えば20円)が、EMDサービスセンタ1の利益である。EMDサービスセンタ1は、ユーザホームネットワーク5のコンテンツの利用結果を示す課金情報(図19(C))とともに、ユーザホームネットワーク5を介して、取扱方針、利益分配率、および価格情報を得ることで、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1のそれぞれの利益を算出できる。

【0077】図20は、コンテンツの再生の利用に、複数の形態が設定されているときの取扱方針、価格情報、および使用許諾条件情報を説明する図である。図20

(A)の例では、サービスプロバイダ3において、取扱方針および価格情報として、コンテンツの再生利用に、制限のない再生、回数制限(この例の場合、5回)のある再生、および期日制限(この例の場合、1998年12月31日まで)のある再生が設定されている。ユーザが、5回の回数制限のある再生を選択して、コンテンツを利用する場合、コンテンツを受け取り、まだ1度も再生していない状態では、図20(B)に示すように、ユーザホームネットワーク5の使用許諾条件情報の回数制限に対応する値には、“5”が記録されている。この回数制限に対応する値は、ユーザホームネットワーク5において、コンテンツが再生(利用)される度にデクリメントされ、例えば、3回再生された後、その値は、図20(C)に示すように“2”とされる。回数制限に対応する値が、“0”となった場合、ユーザホームネットワーク5は、それ以上、そのコンテンツを再生して利用することができない。

【0078】図21は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報の他の例を説明する図である。図12に示した例に対して、図21の例では、サービスプロバイダ3は、コンテンツプロバイダ2からの取扱方針を基に取扱制御情報を作成する。取扱制御情報は、コンテンツなどと共にサービスプロバイダセキュアコンテナに格納され、ユーザホームネ

ットワーク5に送信され、EMDサービスセンタ1にも送受信される。取扱制御情報は、更に、課金情報および取扱方針と共にユーザホームネットワーク5からEMDサービスセンタ1に送信される。

【0079】図22は、図21の例の場合のサービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵Kcoで暗号化されたコンテンツ、配送用鍵Kdで暗号化されたコンテンツ鍵Kco、取扱方針、取扱制御情報、価格情報、および署名を含む。署名は、コンテンツ鍵Kcoで暗号化されたコンテンツ、配送用鍵Kdで暗号化されたコンテンツ鍵Kco、取扱方針、取扱制御情報、および価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵Kssdで暗号化したデータである。

【0080】図23は、図21の例の場合における、取扱方針、取扱制御情報、価格情報、及び使用許諾条件の構成を示す図である。図23に示す例の場合、コンテンツプロバイダ2の取扱方針(図23(A))は、そのまま価格情報を付しても、取扱方針と対比して価格情報を参照できる形式を有しない。そこで、サービスプロバイダ3は、その取扱方針を基に、価格情報と対比して価格情報を参照できる形式を有する取扱制御情報を生成し、それに価格情報を付して、ユーザホームネットワーク5に送信する(図23(B))。ユーザホームネットワークでは、送信を受けた情報から使用許諾条件情報(図23(C))を生成する。図23のコンテンツプロバイダ2は、図12の場合に比較し、より小さいデータ量の取扱方針を記録すればよい利点がある。

【0081】図24は、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信されるコンテンツおよびコンテンツに付随する情報のさらに他の構成を説明する図である。図21に示した例に対して、図24の例では、取扱方針、取扱制御情報、価格情報、および課金情報は、公開鍵暗号により暗号化され、送信される。図24のシステムは、図21の例の場合に比較して、システムの外部からの攻撃に対し、安全性が向上する。

【0082】図25は、図24の例の場合のコンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナは、コンテンツ鍵Kcoで暗号化されたコンテンツ、配送用鍵Kdで暗号化されたコンテンツ鍵Kco、配送用鍵Kdで暗号化された取扱方針、および署名を含む。署名は、コンテンツ鍵Kcoで暗号化されたコンテンツ、配送用鍵Kdで暗号化されたコンテンツ鍵Kco、および配送用鍵Kdで暗号化された取扱方針にハッシュ関数を適用して生成されたハッシュ値を、コンテンツプロバイダ2の秘密鍵Kscdで暗号化したデータである。

【0083】図26は、図24の例の場合のサービスプ

ロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナは、コンテンツ鍵K c oで暗号化されたコンテンツ、配送用鍵K dで暗号化されたコンテンツ鍵K c o、配送用鍵K dで暗号化された取扱方針、配送用鍵K dで暗号化された取扱制御情報、配送用鍵K dで暗号化された価格情報、および署名を含む。署名は、コンテンツ鍵K c oで暗号化されたコンテンツ、配送用鍵K dで暗号化されたコンテンツ鍵K c o、配送用鍵K dで暗号化された取扱方針、配送用鍵K dで暗号化された取扱制御情報、および配送用鍵K dで暗号化された価格情報にハッシュ関数を適用して生成されたハッシュ値を、サービスプロバイダ3の秘密鍵K s s pで暗号化したデータである。

【0084】図27は、EMDサービスセンタ1が、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5から、決算処理に必要なデータを収集する他の動作を説明する図である。コンテンツプロバイダ2は、EMDサービスセンタ1に、コンテンツプロバイダ2の名前、コンテンツID、コンテンツIDに対応する権利団体の利益、およびコンテンツプロバイダ2の銀行口座番号などのデータからなるコンテンツプロバイダ登録データを送信し、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ登録データを受信する。EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ登録データを受信したとき、コンテンツプロバイダIDを生成し、コンテンツプロバイダIDとともにコンテンツプロバイダ登録データを利益配分データベースに登録し、コンテンツプロバイダIDをコンテンツプロバイダ2に送信する。コンテンツプロバイダ2は、コンテンツプロバイダIDを受信し、記憶する。

【0085】サービスプロバイダ3は、EMDサービスセンタ1にサービスプロバイダ3の名前、コンテンツID、およびサービスプロバイダ3の銀行口座番号などのデータからなるサービスプロバイダ登録データを送信し、EMDサービスセンタ1のサービスプロバイダ管理部11は、サービスプロバイダ登録データを受信する。EMDサービスセンタ1のサービスプロバイダ管理部11は、サービスプロバイダ登録データを受信したとき、サービスプロバイダIDを生成し、サービスプロバイダIDをサービスプロバイダ3に送信する。サービスプロバイダ3は、コンテンツプロバイダIDを受信し、記憶する。

【0086】ユーザホームネットワーク5は、EMDサービスセンタ1にユーザの名前、ユーザの銀行口座番号などのデータからなるユーザ登録データを送信し、EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データを受信する。EMDサービスセンタ1のユーザ管理部18は、ユーザ登録データの受信により、ユーザIDを生成し、ユーザIDとともにユーザ登録データを記憶し、ユーザIDをユーザホームネットワーク5に送信する。ユーザ

ホームネットワーク5は、ユーザIDを受信し、記憶する。

【0087】図28は、利益配分データベースの例を示す図である。利益配分データベースは、コンテンツIDに対応する権利団体への配分が記憶されている。コンテンツIDに対応する権利団体への配分は、権利団体への、コンテンツIDに対応するコンテンツがユーザに利用されたときに発生する利益の配分の割合を示す。

【0088】図28に示す利益配分データベースの例において、コンテンツIDが1であるコンテンツがサービスプロバイダ3からユーザに提供された場合、権利団体には、コンテンツがユーザに利用されることによる利益の10%が配分される。同様に、コンテンツIDが2であるコンテンツがユーザに利用されることによる利益の20%は、権利団体に配分される。

【0089】図29は、EMDサービスセンタ1の利益配部16が記憶するコンテンツの利用料金の割引テーブルの例を示す図である。コンテンツの利用料金の割引テーブルには、コンテンツIDおよびコンテンツプロバイダIDに対応するユーザの利用料金の割引率が格納されている。割引テーブルには、割引率を、適用する期間の情報なども格納できるようになされている。

【0090】コンテンツプロバイダIDが1であるコンテンツプロバイダ2が供給するコンテンツIDが1であるコンテンツの利用料金は、1998年9月から1998年12月までの間、0.02割引かれる。コンテンツプロバイダIDが1であるコンテンツプロバイダ2が供給するコンテンツIDが2であるコンテンツの利用料金は、0.03割引かれる。コンテンツプロバイダIDが1であるコンテンツプロバイダ2が供給するコンテンツIDが1または2以外であるコンテンツの利用料金は、0.01割引かれる。コンテンツプロバイダIDが2であるコンテンツプロバイダ2が供給するコンテンツIDが3であるコンテンツの利用料金は、0.05割引かれる。サービスプロバイダIDが1であるサービスプロバイダ3が提供するコンテンツIDが1であるコンテンツの利用料金は、0.03割引かれる。サービスプロバイダIDが2であるサービスプロバイダ3が提供するコンテンツIDが4であるコンテンツの利用料金は、0.01割引かれる。

【0091】図30は、EMDサービスセンタ1の課金請求部19が記憶する、ユーザに対するEMDサービスセンタ1の利用料金を格納するユーザ利用料金テーブルの例を示している。ユーザ利用料金テーブルの月額固定額は、ユーザがEMDサービスセンタ1に毎月支払う一定の利用料金の額を表す。変動額は、EMDサービスセンタ1特別に定めた所定の期間の月額固定額の割引率、または、コンテンツの利用料金を含めた利用料が所定の額以上である場合の月額固定額の割引率を表す。

【0092】図30に示すユーザ利用料金テーブルの例

において、月額固定額は、1000円であり、1998年8月から1998年9月の間、月額固定額は、10%割引かれる。また、コンテンツの利用料金を含めた利用料が3000円以上である場合、月額固定額は、5%割引かれる。

【0093】利益配分データベースまたは課金情報からコンテンツの利用料金が算出され、コンテンツの利用料金から割引テーブルに基づく割引額が減算され、ユーザ利用料金テーブルに格納されているEMDサービスセンタ1の利用料金が加算されて、ユーザの利用料金が、算出される。

【0094】図31は、EMDサービスセンタ1が、ユーザホームネットワーク5から課金情報を受信するときの動作を説明する図である。ユーザホームネットワーク5と相互認証した後、ユーザ管理部18は、一時鍵Ktempを共有化し、鍵サーバ14からの配送用鍵Kdをこの鍵で暗号化しユーザホームネットワーク5に送信する。ユーザホームネットワーク5は、受信した配送用鍵Kdを共有化した一時鍵Ktempで復号化した後、配送用鍵Kdを必要に応じて更新する。また、共有化した一時鍵Ktempを用いて課金情報、および取扱方針等を暗号化し、EMDサービスセンタ1に送信する。ユーザ管理部18はこれを受信する。ユーザ管理部18は、受信した課金情報、および取扱方針等を共有化した一時鍵Ktempで復号化した後、経歴データ管理部15および課金請求部19に送信する。経歴データ管理部15は決済を実行すると判定した場合、受信した課金情報を利益分配部16に送信し、さらに、受信した課金情報および取扱方針等を課金請求部19に送信する。利益分配部16は、利益配分データベース、および割引テーブルを基に、図57で説明する処理で、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1自身に対する請求金額および支払金額を算出する。課金請求部19は、ユーザ利用料金テーブルを基に、ユーザへの請求金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。その際、ユーザの料金の未払い等の情報があれば、それらの情報は、課金請求部19およびユーザ管理部18に送信され、以後のユーザの登録処理時、または配送用鍵Kdの送信処理時に参照される。

【0095】図32は、EMDサービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報、取扱方針、および価格データを利益分配部16に送信する。利益分配部16は、これらの情報を基に、コンテンツプロバイダ2、サービスプロバイダ3、およびEMDサービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に送信する。出納部20は、図示せぬ外部の銀行等と通信し、

決算処理を実行する。サービスプロバイダ管理部11は、サービスプロバイダ3の利益の情報をサービスプロバイダ3に送信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2の利益の情報をコンテンツプロバイダ2に送信する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針の正当性を監査する。

【0096】図33は、EMDサービスセンタ1の、コンテンツの利用実績の情報をJASRACに送信する処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの使用実績を示す課金情報を著作権管理部13および利益分配部16に送信する。利益分配部16は、利益配分データベース、および割引テーブルを基に、図57で説明する処理で、JASRACに対する請求金額および支払金額を算出し、その情報を出納部20に送信する。出納部20は、図示せぬ外部の銀行等と通信し、決算処理を実行する。著作権管理部13は、ユーザのコンテンツの使用実績をJASRACに送信する。

【0097】次に、EMDシステムの処理について説明する。図34は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップS11において、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信し、コンテンツプロバイダ2がこれを受信する。その処理の詳細は、図36のフローチャートを参照して後述する。ステップS12において、ユーザは、ユーザホームネットワーク5の機器（例えば、図10のレシーバ51）を操作し、ユーザホームネットワーク5の機器をEMDサービスセンタ1のユーザ管理部18に登録する。この登録処理の詳細は、図40のフローチャートを参照して後述する。ステップS13において、EMDサービスセンタ1のユーザ管理部18は、ユーザホームネットワーク5と、図37乃至図39に示したように相互認証した後、ユーザホームネットワーク5の機器に、配送用鍵Kdを送信する。ユーザホームネットワーク5はこの鍵を受信する。この処理の詳細は、図48のフローチャートを参照して説明する。

【0098】ステップS14において、コンテンツプロバイダ2のセキュアコンテンツ作成部38は、サービスプロバイダ3にコンテンツプロバイダセキュアコンテンツを送信する。この送信処理の詳細は、図50のフローチャートを参照して後述する。ステップS15において、サービスプロバイダ3のセキュアコンテンツ作成部44は、ユーザホームネットワーク5からの要求に応じて、ネットワーク4を介して、ユーザホームネットワーク5にサービスプロバイダセキュアコンテンツを送信する。この送信処理の詳細は、図52のフローチャートを参照して後述する。ステップS16において、ユーザホームネットワーク5の課金モジュール72は、課金処理を実行する。課金処理の詳細は、図54のフローチャートを参照

して後述する。ステップS 17において、ユーザは、ユーザホームネットワーク 5の機器でコンテンツを再生する。再生処理の詳細は、図 5 5のフローチャートを参照して後述する。

【0099】一方、コンテンツプロバイダ 2が、取扱方針を暗号化して送信する場合の処理は、図 3 5のフローチャートで示すようになる。ステップS 21において、EMDサービスセンタ 1のコンテンツプロバイダ管理部 12は、コンテンツプロバイダ 2に配送用鍵K dを送信する。ステップS 22において、EMDサービスセンタ 1のサービスプロバイダ管理部 11は、サービスプロバイダ 3に配送用鍵K dを送信する。それ以降のステップS 23乃至ステップS 28の処理は、図 3 4のステップS 12乃至ステップS 17の処理と同様の処理であり、その説明は省略する。

【0100】図 3 6は、図 3 4のステップS 11および図 3 5のステップS 21に対応する、EMDサービスセンタ 1がコンテンツプロバイダ 2へ配送用鍵K dを送信し、コンテンツプロバイダ 2がこれを受信する処理の詳細を説明するフローチャートである。ステップS 31において、EMDサービスセンタ 1の相互認証部 17は、コンテンツプロバイダ 2の相互認証部 39と相互認証する。この相互認証処理の詳細は、図 3 7を参照して後述する。相互認証処理により、コンテンツプロバイダ 2が、正当なプロバイダであることが確認されたとき、ステップS 32において、コンテンツプロバイダ 2の暗号化部 34および暗号化部 36は、EMDサービスセンタ 1のコンテンツプロバイダ管理部 12から送信された配送用鍵K dを受信する。ステップS 33において、コンテンツプロバイダ 2の暗号化部 34は、受信した配送用鍵K dを記憶する。

【0101】このように、コンテンツプロバイダ 2は、EMDサービスセンタ 1から配送用鍵K dを受け取る。同様に、図 3 5に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ 2以外に、サービスプロバイダ 3も、図 3 6と同様の処理で、EMDサービスセンタ 1から配送用鍵K dを受け取る。

【0102】次に、図 3 6のステップS 31における、いわゆるなりすましが無いことを確認する相互認証の処理について、1つの共通鍵を用いる（図 3 7）、2つの共通鍵を用いる（図 3 8）、および公開鍵暗号を用いる（図 3 9）を例として説明する。

【0103】図 3 7は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ 2の相互認証部 39とEMDサービスセンタ 1の相互認証部 17との相互認証の動作を説明するフローチャートである。ステップS 41において、コンテンツプロバイダ 2の相互認証部 39は、64ビットの乱数R 1を生成する（乱数生成部 35が生成するようにしてもよい）。ステップS 42において、コンテンツプロバイダ 2の相互認証部 39

は、DESを用いて乱数R 1を、予め記憶している共通鍵K cで暗号化する（暗号化部 36で暗号化するようにしてもよい）。ステップS 43において、コンテンツプロバイダ 2の相互認証部 39は、暗号化された乱数R 1をEMDサービスセンタ 1の相互認証部 17に送信する。

【0104】ステップS 44において、EMDサービスセンタ 1の相互認証部 17は、受信した乱数R 1を予め記憶している共通鍵K cで復号する。ステップS 45において、EMDサービスセンタ 1の相互認証部 17は、32ビットの乱数R 2を生成する。ステップS 46において、EMDサービスセンタ 1の相互認証部 17は、復号した64ビットの乱数R 1の下位32ビットを乱数R 2に入れ替え、接続R 1_{||}R 2を生成する。なお、ここでR i_{||}は、R iの上位ビットを表し、A_{||}Bは、AとBの接続（nビットのAの下位に、mビットのBを結合して、（n+m）ビットとしたもの）を表す。ステップS 47において、EMDサービスセンタ 1の相互認証部 17は、DESを用いてR 1_{||}R 2を共通鍵K cで暗号化する。ステップS 48において、EMDサービスセンタ 1の相互認証部 17は、暗号化したR 1_{||}R 2をコンテンツプロバイダ 2に送信する。

【0105】ステップS 49において、コンテンツプロバイダ 2の相互認証部 39は、受信したR 1_{||}R 2を共通鍵K cで復号する。ステップS 50において、コンテンツプロバイダ 2の相互認証部 39は、復号したR 1_{||}R 2の上位32ビットR 1_{||}を調べ、ステップS 41で生成した、乱数R 1の上位32ビットR 1_{||}と一致すれば、EMDサービスセンタ 1が正当なセンタであることを認証する。生成した乱数R 1_{||}と、受信したR 1_{||}が一致しないとき、処理は終了される。両者が一致するとき、ステップS 51において、コンテンツプロバイダ 2の相互認証部 39は、32ビットの乱数R 3を生成する。ステップS 52において、コンテンツプロバイダ 2の相互認証部 39は、受信し、復号した32ビットの乱数R 2を上位に設定し、生成した乱数R 3をその下位に設定し、接続R 2_{||}R 3とする。ステップS 53において、コンテンツプロバイダ 2の相互認証部 39は、DESを用いて接続R 2_{||}R 3を共通鍵K cで暗号化する。ステップS 54において、コンテンツプロバイダ 2の相互認証部 39は、暗号化された接続R 2_{||}R 3をEMDサービスセンタ 1の相互認証部 17に送信する。

【0106】ステップS 55において、EMDサービスセンタ 1の相互認証部 17は、受信した接続R 2_{||}R 3を共通鍵K cで復号する。ステップS 56において、EMDサービスセンタ 1の相互認証部 17は、復号した接続R 2_{||}R 3の上位32ビットを調べ、乱数R 2と一致すれば、コンテンツプロバイダ 2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0107】図 3 8は、2つの共通鍵K c 1、K c 2

で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を予め記憶している共通鍵Kc1で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1に送信する。

【0108】ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kc1で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数R1を予め記憶している共通鍵Kc2で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数R2を共通鍵Kc2で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数R1および乱数R2をコンテンツプロバイダ2の相互認証部39に送信する。

【0109】ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数R1および乱数R2を予め記憶している共通鍵Kc2で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数R1を調べ、ステップS61で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数R2を共通鍵Kc1で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R2をEMDサービスセンタ1に送信する。

【0110】ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R2を共通鍵Kc1で復号する。ステップS74において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS66で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0111】図39は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS81において、コンテンツプロバイダ2

の相互認証部39は、64ビットの乱数R1を生成する。ステップS82において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵Kpcpを含む証明書（認証局から予め取得しておいたもの）と、乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

【0112】ステップS83において、EMDサービスセンタ1の相互認証部17は、受信した証明書の署名（認証局の秘密鍵Kscaで暗号化されている）を、予め取得しておいた認証局の公開鍵Kpcaで復号し、コンテンツプロバイダ2の公開鍵Kpcpとコンテンツプロバイダ2の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ2の公開鍵Kpcpおよびコンテンツプロバイダ2の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Kpcpおよびコンテンツプロバイダ2の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ2の公開鍵Kpcpおよびコンテンツプロバイダ2の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Kpcpが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0113】適正な認証結果が得られたとき、ステップS84において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS85において、EMDサービスセンタ1の相互認証部17は、乱数R1および乱数R2の接続R1||R2を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続R1||R2を自分自身の秘密鍵Ksescで暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続R1||R2を、ステップS83で取得したコンテンツプロバイダ2の公開鍵Kpcpで暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵Ksescで暗号化された接続R1||R2、公開鍵Kpcpで暗号化された接続R1||R2、および自分自身の公開鍵Kpescを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相互認証部39に送信する。

【0114】ステップS89において、コンテンツプロバイダ2の相互認証部39は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Kpcaで復号し、正しければ証明書から公開鍵Kpescを取り出す。この場合の処理は、ステップS83における場合と同様であるので、その説明は省略する。ステップS90において、コンテンツプロバイダ2の相互認証部39は、EMD

サービスセンタ1の秘密鍵K s e s cで暗号化されている接続R 1 || R 2を、ステップS 8 9で取得した公開鍵K p e s cで復号する。ステップS 9 1において、コンテンツプロバイダ2の相互認証部3 9は、自分自身の公開鍵K p c pで暗号化されている接続R 1 || R 2を、自分自身の秘密鍵K s c pで復号する。ステップS 9 2において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で復号された接続R 1 || R 2と、ステップS 9 1で復号された接続R 1 || R 2を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0 1 1 5】適正な認証結果が得られたとき、ステップS 9 3において、コンテンツプロバイダ2の相互認証部3 9は、6 4ビットの乱数R 3を生成する。ステップS 9 4において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で取得した乱数R 2および生成した乱数R 3の接続R 2 || R 3を生成する。ステップS 9 5において、コンテンツプロバイダ2の相互認証部3 9は、接続R 2 || R 3を、ステップS 8 9で取得した公開鍵K p e s cで暗号化する。ステップS 9 6において、コンテンツプロバイダ2の相互認証部3 9は、暗号化した接続R 2 || R 3をEMDサービスセンタ1の相互認証部1 7に送信する。

【0 1 1 6】ステップS 9 7において、EMDサービスセンタ1の相互認証部1 7は、暗号化された接続R 2 || R 3を自分自身の秘密鍵K s e s cで復号する。ステップS 9 8において、EMDサービスセンタ1の相互認証部1 7は、復号した乱数R 2が、ステップS 8 4で生成した乱数R 2（暗号化する前の乱数R 2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0 1 1 7】以上のように、EMDサービスセンタ1の相互認証部1 7とコンテンツプロバイダ2の相互認証部3 9は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵K t e m pとして利用される。

【0 1 1 8】図4 0は、図3 4のステップS 1 2および図3 5のステップS 2 3に対応する、レシーバ5 1がEMDサービスセンタ1のユーザ管理部1 8に登録する処理を説明するフローチャートである。ステップS 1 0 1において、レシーバ5 1のSAM 6 2は、ICカードインターフェース6 4の出力から、レシーバ5 1にバックアップ用のICカード5 5が装着されているか否かを判定し、バックアップ用のICカード5 5が装着されていると判定された場合（例えば、レシーバ5 1が新たなレシーバ5 1に変更され、元のレシーバ5 1のデータを、新たなレシーバ5 1に引き継ぐために、元のレシーバ5 1のデータをバックアップ用のICカード5 5にバックアップさせて

いる場合）、ステップS 1 0 2に進み、ICカード5 5に記憶されているバックアップデータの読み込み処理を実行する。この処理の詳細は、図4 5のフローチャートを参照して後述する。勿論、この読み込み処理が実行されるためには、その前に、ICカード5 5に、バックアップデータを記憶させる必要があるが、その処理は、図4 3を参照して後述する。

【0 1 1 9】ステップS 1 0 1において、バックアップ用のICカード5 5が装着されていないと判定された場合、手続は、ステップS 1 0 2をスキップし、ステップS 1 0 3に進む。ステップS 1 0 3において、SAM 6 2の相互認証モジュール7 1は、EMDサービスセンタ1の相互認証部1 7と相互認証し、SAM 6 2は、証明書をEMDサービスセンタ1のユーザ管理部1 8に送信する。この認証処理は、図3 7乃至図3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 0 3で、SAM 6 2がEMDサービスセンタ1のユーザ管理部1 8に送信する証明書は、図4 1に示すデータを含む。SAM 6 2が送信する証明書は、図1 4に示すコンテンツプロバイダ2の証明書とほぼ同様の構成を有するが、更に、他のSAMに従属するか否かを示すデータを含んでいる。ステップS 1 0 4において、SAM 6 2は、通信部6 1を介して、一時鍵K t e m pで暗号化した、ユーザの銀行等の決済機関の情報等をEMDサービスセンタ1のユーザ管理部1 8に送信する。

【0 1 2 0】ステップS 1 0 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信したSAM 6 2のIDを基に、図7に示したユーザ登録データベースを検索する。ステップS 1 0 6において、EMDサービスセンタ1のユーザ管理部1 8は、受信したIDを有するSAM 6 2の登録が可能であるか否かを判定し、受信したIDを有するSAM 6 2の登録が可能であると判定された場合、ステップS 1 0 7に進み、受信したIDを有するSAM 6 2が、新規登録であるか否かを判定する。ステップS 1 0 7において、受信したIDを有するSAM 6 2が、新規登録ではないと判定された場合、手続は、ステップS 1 0 8に進む。

【0 1 2 1】ステップS 1 0 8において、EMDサービスセンタ1のユーザ管理部1 8は、更新登録を実行し、受信したIDを基にユーザ登録データベースを検索し、登録リストを作成する。この登録リストは、例えば、図4 2に示す構造を有し、機器のSAMのIDに対応して、EMDサービスセンタ1のユーザ管理部1 8が登録を拒絶したか否かを示す登録拒絶フラグ、従属する機器である場合のコンテンツ鍵K c oの利用条件を示すステータスフラグ、従属する機器であるか否かを示すコンディションフラグ、並びに登録拒絶フラグ、ステータスフラグ、およびコンディションフラグにハッシュ関数を適用して生成したハッシュ値をEMDサービスセンタ1の秘密鍵K s e s cで暗号化した署名から構成される。

【0122】機器のSAMのIDは、機器の固有の64ビットからなるIDを示す(図42では、16進数で示す)。登録拒絶フラグの"1"は、EMDサービスセンタ1のユーザ管理部18が対応するIDを有する機器を登録したことを示し、登録拒絶フラグの"0"は、MDサービスセンタ1のユーザ管理部18が対応するIDを有する機器の登録を拒絶したことを示す。

【0123】ステータスフラグのMSB(Most Significant Bit)の"1"は、対応するIDを有する子の機器(例えばレコーダ53)が従属した親の機器(例えばレシーバ51)からコンテンツ鍵Kcoをもらえることを示し、ステータスフラグのMSBの"0"は、対応するIDを有する子の機器が従属した親の機器からコンテンツ鍵Kcoをもらえないことを示している。ステータスフラグの上位から2ビット目の"1"は、対応するIDを有する子の機器が従属した親の機器から、親の機器の保存用鍵Ksaveで暗号化されたコンテンツ鍵Kcoをもらえることを示す。ステータスフラグの上位から3ビット目の"1"は、対応するIDを有する子の機器が従属した親の機器から、配送用鍵Kdで暗号化されたコンテンツ鍵Kcoをもらえることを示す。ステータスフラグのLSB(Least Significant Bit)の"1"は、従属した親の機器が配送用鍵Kdで暗号化したコンテンツ鍵Kcoを購入し、対応するIDを有する子の機器に、一時鍵Ktempで暗号化してコンテンツ鍵Kcoを渡すことを示す。

【0124】コンディションフラグの"0"は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来る(すなわち、例えばレシーバ51のような親の機器である)ことを示し、コンディションフラグの"1"は、対応するIDを有する機器がEMDサービスセンタ1のユーザ管理部18と直接通信が出来ない(すなわち、例えばレコーダ53のような子の機器である)ことを示す。コンディションフラグが"0"のとき、ステータスフラグは常に"0000"に設定される。

【0125】ステップS109において、EMDサービスセンタ1のユーザ管理部18は、相互認証部17から供給された一時鍵Ktempで暗号化した、鍵サーバ14から供給された配送用鍵Kdをレシーバ51のSAM62に送信する。ステップS110において、レシーバ51のSAM62は、受信した配送用鍵Kdを一時鍵Ktempで復号し、記憶モジュール73に記憶させる。

【0126】ステップS111において、EMDサービスセンタ1のユーザ管理部18は、一時鍵Ktempで暗号化した登録リストをレシーバ51のSAM62に送信する。ステップS112において、レシーバ51のSAM62は、受信した登録リストを一時鍵Ktempで復号し、記憶モジュール73に記憶させ、処理は終了する。

【0127】ステップS107において、受信したIDを有するSAM62が、新規登録であると判定された場合、

手続は、ステップS114に進み、EMDサービスセンタ1のユーザ管理部18は、新規登録を実行し、登録リストを作成し、ステップS109に進む。

【0128】ステップS106において、受信したIDを有するSAM62の登録が不可であると判定された場合、ステップS113に進み、EMDサービスセンタ1のユーザ管理部18は、登録拒絶の登録リストを作成し、ステップS111に進む。

【0129】このように、レシーバ51は、EMDサービスセンタ1に登録される。

【0130】次に、今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵Kdなどの所定のデータをICカード55に記憶させる処理の詳細を、図43のフローチャートを参照して説明する。ステップS121において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS122において、SAM62の乱数発生ユニット92は、バックアップ鍵Kicとして用いられる乱数を生成する。ステップS123において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵Ksave、およびHDD52のIDを、バックアップ鍵Kicを用いて暗号化する。ステップS124において、SAM62の暗号化ユニット93は、EMDサービスセンタ1の公開鍵Kpescでバックアップ鍵Kicを暗号化する(SAM62は、EMDサービスセンタ1との間の認証処理(図39のステップS89)において、EMDサービスセンタ1の公開鍵Kpescを取得している)。ステップS125において、レシーバ51のSAM62は、ICカードインターフェース64を介して、暗号化されたSAMのID番号、保存用鍵Ksave、およびHDD52のID並びに暗号化されたバックアップ鍵KicをICカード55に送信し、記憶モジュール81に記憶させる。

【0131】以上のように、SAM62の記憶モジュール73に記憶されたSAMのID番号、保存用鍵Ksave、およびHDD52のIDは、バックアップ鍵Kicを用いて暗号化され、EMDサービスセンタ1の公開鍵Kpescを用いて暗号化されたバックアップ鍵Kicと共に、ICカード55の記憶モジュール81に記憶される。

【0132】今まで使用していたレシーバ51の記憶モジュール73に記憶された配送用鍵Kdなどの所定のデータをICカード55に記憶させる他の処理の例の詳細を、図44のフローチャートを参照して説明する。ステップS131において、SAM62の相互認証モジュール71は、ICカード55の相互認証モジュール80と相互認証する。ステップS132において、SAM62の暗号化ユニット93は、記憶モジュール73に記憶されているSAMのID番号、保存用鍵Ksave、およびHDD52の

IDを、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化する。ステップS 1 3 3において、レシーバ51のSAM6 2は、ICカードインタフェース6 4を介して、暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD5 2のIDをICカード5 5に送信し、記憶モジュール8 1に記憶させる。

【0133】図4 4に示す処理により、図4 3に示した場合より簡単な処理で、EMDサービスセンタ1の公開鍵K p e s cを用いて暗号化されたSAMのID番号、保存用鍵K s a v e、およびHDD5 2のIDは、ICカード5 5の記憶モジュール8 1に記憶される。

【0134】このように、ICカード5 5にバックアップされたデータは、図4 0のステップS 1 0 2の処理で、新しいレシーバ5 1に読み込まれる。図4 5は、図4 3に示す処理でバックアップされたデータ読み出す場合の処理を説明するフローチャートである。ステップS 1 4 1において、新しいレシーバ5 1のSAM6 2の相互認証モジュール7 1は、ICカード5 5の相互認証モジュール8 0と相互認証する。この認証処理は、図3 7乃至図3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0135】ステップS 1 4 2において、SAM6 2は、ICカードインタフェース6 4を介して、記憶モジュール8 1に記憶された、バックアップ鍵K i cで暗号化されている古いレシーバ5 1の記憶モジュール7 3のデータ（SAMのID番号、保存用鍵K s a v e、およびHDD5 2のIDを示すバックアップデータ）、およびEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを読み出す。ステップS 1 4 3において、SAM6 2の相互認証モジュール7 1は、通信部6 1を介して、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図3 7乃至図3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 4 4において、SAM6 2は、通信部6 1を介して、バックアップ鍵K i cで暗号化されている記憶モジュール7 3のデータ、およびEMDサービスセンタ1の公開鍵K p e s cで暗号化されているバックアップ鍵K i cを、EMDサービスセンタ1のユーザ管理部1 8に送信する。

【0136】ステップS 1 4 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップ鍵K i cを自分自身の秘密鍵K s e s cで復号する。ステップS 1 4 6において、EMDサービスセンタ1のユーザ管理部1 8は、受信したバックアップデータを、バックアップ鍵K i cで復号する。ステップS 1 4 7において、EMDサービスセンタ1のユーザ管理部1 8は、復号したバックアップデータを、相互認証部1 7から供給された一時鍵K t e m pで、再度、暗号化する。ステップS 1 4 8において、EMDサービスセンタ1のユーザ管理部1 8は、一時鍵K t e m pで暗号化されたバックアッ

プデータを、レシーバ5 1の通信部6 1に送信する。

【0137】ステップS 1 4 9において、レシーバ5 1の通信部6 1は、EMDサービスセンタ1のユーザ管理部1 8から受信したデータを、SAM6 2に送信し、SAM6 2は、そのデータを復号した後、記憶モジュール7 3に記憶させる。ステップS 1 5 0において、EMDサービスセンタ1のユーザ管理部1 8は、ICカード5 5にデータを記憶させた古い装置のSAM6 2のIDに対応するユーザ登録データベース（図7）のデータを登録不可に設定し、処理を終了する。

【0138】このように、新しいレシーバ5 1は、ICカード5 5のバックアップデータを読み込む。

【0139】図4 4に示す処理でバックアップされたデータ読み出す場合の処理を、図4 6に示すフローチャートを用いて説明する。ステップS 1 6 1において、新しいレシーバ5 1のSAM6 2の相互認証モジュール7 1は、ICカード5 5の相互認証モジュール8 0と相互認証する。この認証処理は、図3 7乃至図3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 6 2において、SAM6 2は、ICカードインタフェース6 4を介して、EMDサービスセンタ1の公開鍵K p e s cで暗号化されている古いレシーバ5 1の記憶モジュール7 3のデータ（SAMのID番号、保存用鍵K s a v e、およびHDD5 2のIDを示すバックアップデータ）を読み出す。

【0140】ステップS 1 6 3において、SAM6 2の相互認証モジュール7 1は、通信部6 1を介して、EMDサービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図3 7乃至図3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 1 6 4において、SAM6 2は、通信部6 1を介して、EMDサービスセンタ1の公開鍵K p e s cで暗号化されている記憶モジュール7 3のデータを、EMDサービスセンタ1のユーザ管理部1 8に送信する。

【0141】ステップS 1 6 5において、EMDサービスセンタ1のユーザ管理部1 8は、受信した記憶モジュール7 3のデータを自分自身の秘密鍵K s e s cで復号する。ステップS 1 6 6において、EMDサービスセンタ1のユーザ管理部1 8は、復号したバックアップデータを、相互認証部1 7から供給された一時鍵K t e m pで、再度、暗号化する。ステップS 1 6 7において、EMDサービスセンタ1のユーザ管理部1 8は、一時鍵K t e m pで暗号化されたバックアップデータを、レシーバ5 1の通信部6 1に送信する。

【0142】ステップS 1 6 8において、レシーバ5 1の通信部6 1は、EMDサービスセンタ1のユーザ管理部1 8から受信したデータを、SAM6 2に送信し、SAM6 2は、そのデータを復号した後、記憶モジュール7 3に記憶させる。ステップS 1 6 9において、EMDサービスセンタ1のユーザ管理部1 8は、ICカード5 5にデータ

を記憶させた古い装置のSAM 6 2のIDに対応するユーザ登録データベース（図 7）のデータを登録不可に設定する。

【0143】このように、図 4 4に示す処理を用いたバックアップの場合、図 4 6に示す処理により、新しいレシーバ 5 1は、ICカード 5 5のバックアップデータを読み込む。

【0144】レシーバ 5 1は、自分自身を登録する場合（図 3 4のステップ S 1 2に対応する処理を実行する場合）、図 4 0のフローチャートに示す処理を実行するが、レシーバ 5 1に従属するレコーダ 5 3をEMDサービスセンタ 1に登録する場合、図 4 7のフローチャートに示す処理を実行する。ステップ S 1 8 1において、レシーバ 5 1のSAM 6 2は、記憶モジュール 7 3に記憶された登録リストに、レコーダ 5 3のIDを書き込む。ステップ S 1 8 2において、レシーバ 5 1の相互認証モジュール 7 1は、EMDサービスセンタ 1の相互認証部 1 7と相互認証する。この認証処理は、図 3 7乃至図 3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0145】ステップ S 1 8 3において、EMDサービスセンタ 1のユーザ管理部 1 8は、レシーバ 5 1のID（図 4 1に示すSAM 6 2の証明書に含まれるSAM 6 2のID）を基に、ユーザ登録データベースを検索し、レシーバ 5 1が登録不可であるか否かを判定し、レシーバ 5 1が登録不可ではないと判定された場合、ステップ S 1 8 4に進み、レシーバ 5 1のSAM 6 2は、EMDサービスセンタ 1のユーザ管理部 1 8に、記憶モジュール 7 3に記憶している配送用鍵 K dのバージョン、課金情報（後述の図 5 4に示すフローチャートのステップ S 3 3 7の処理で記憶される）、および登録リスト、並びにHDD 5 2に記録された取扱方針を一時鍵 K dで暗号化し、通信部 6 1を介して、EMDサービスセンタ 1のユーザ管理部 1 8に、記憶モジュール 7 3に記憶している配送用鍵 K dのバージョン、課金情報、および登録リスト、並びにHDD 5 2に記録された取扱方針を送信する。ステップ S 1 8 5において、EMDサービスセンタ 1のユーザ管理部 1 8は、受信したデータを復号した後、課金情報を処理し、図 4 2を参照して説明した、レシーバ 5 1から受信した登録リストのレコーダ 5 3に関する登録拒絶フラグ、およびステータスフラグなどのデータの部分を更新し、レシーバ 5 1に対応するデータに応じた署名を付する。

【0146】ステップ S 1 8 6において、EMDサービスセンタ 1のユーザ管理部 1 8は、レシーバ 5 1が有する配送用鍵 K dのバージョンが最新か否かを判定し、レシーバ 5 1が有する配送用鍵 K dのバージョンが最新であると判定された場合、ステップ S 1 8 7に進み、一時鍵 K dで暗号化した、更新した登録リスト、および課金情報受信メッセージを、レシーバ 5 1に送信し、レシーバ 5 1は、更新した登録リスト、および課金情報受信メッ

セージを受信し、復号した後、記憶する。ステップ S 1 8 8において、レシーバ 5 1は、記憶モジュール 7 3に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ 1のユーザ管理部 1 8からステップ S 1 8 7において受信したものに更新し、ステップ S 1 9 1に進む。

【0147】ステップ S 1 8 6において、レシーバ 5 1が有する配送用鍵 K dのバージョンが最新のものではないと判定された場合、ステップ S 1 8 9に進み、EMDサービスセンタ 1のユーザ管理部 1 8は、一時鍵 K dで暗号化した、最新バージョンの配送用鍵 K d、更新した登録リスト、および課金情報受信メッセージを、レシーバ 5 1に送信し、レシーバ 5 1は、最新バージョンの配送用鍵 K d、更新した登録リスト、および課金情報受信メッセージを受信し、復号した後、記憶する。ステップ S 1 9 0において、レシーバ 5 1は、記憶モジュール 7 3に記憶された課金情報を消去し、登録リストを、EMDサービスセンタ 1のユーザ管理部 1 8からステップ S 1 8 9において受信したものに更新し、配送用鍵 K dを最新バージョンのものに更新し、ステップ S 1 9 1に進む。

【0148】ステップ S 1 9 1において、レシーバ 5 1のSAM 6 2は、更新した登録リストを参照し、レコーダ 5 3が登録不可か否かを判定し、レコーダ 5 3が登録不可でないと判定された場合、ステップ S 1 9 2に進み、レシーバ 5 1とレコーダ 5 3は相互認証し、一時鍵 K t empを共有する。この認証処理は、図 3 7乃至図 3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 1 9 3において、レコーダ 5 3に、一時鍵 K dで暗号化した、登録完了メッセージ、および配送用鍵 K dを送信し、レコーダ 5 3は、登録完了メッセージ、および配送用鍵 K dを受信し、復号する。ステップ S 1 9 4において、レコーダ 5 3は、配送用鍵 K dを更新し、処理は終了する。

【0149】ステップ S 1 8 3において、レシーバ 5 1が登録不可であると判定された場合、および、ステップ S 1 9 1において、レコーダ 5 3が登録不可であると判定された場合、処理は終了する。

【0150】以上のように、レシーバ 5 1に従属するレコーダ 5 3は、レシーバ 5 1を介して、EMDサービスセンタ 1に登録される。

【0151】図 4 8は、図 3 4のステップ S 1 3において、EMDサービスセンタ 1がレシーバ 5 1に送信した配送用鍵 K dを、レシーバ 5 1が受け取る処理の詳細を説明するフローチャートである。ステップ S 2 0 1において、レシーバ 5 1の相互認証モジュール 7 1は、EMDサービスセンタ 1の相互認証部 1 7と相互認証する。この認証処理は、図 3 7乃至図 3 9を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 2 0 2において、レシーバ 5 1のSAM 6 2は、通信部 6 1を介して、EMDサービスセンタ 1のユーザ管理部 1

8に証明書を送信し、EMDサービスセンタ1のユーザ管理部18は、証明書を受信する。ステップS203乃至ステップS210は、図47のステップS183乃至ステップS190と同様の処理であるのでその説明は省略する。

【0152】このように、レシーバ51は、EMDサービスセンタ1のユーザ管理部18から配送用鍵Kdを受け取り、レシーバ51の課金情報をEMDサービスセンタ1のユーザ管理部18に送信する。

【0153】次に、レシーバ51に従属するレコーダ53の配送用鍵Kdの受け取り処理（図42に示すステータスフラグが、レコーダ53の配送用鍵Kdの受け取りを許可する値を有する場合）を、図49に示すフローチャートを用いて説明する。ステップS221において、レシーバ51の相互認証モジュール71およびレコーダ53の図示せぬ相互認証モジュールは、相互認証する。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。

【0154】ステップS222において、レシーバ51は、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っているか否かを判定し、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていると判定された場合、ステップS223に進み、レシーバ51の記憶モジュール73に記憶する登録リストを基に、レコーダ53が登録不可であるか否かを判定する。ステップS223において、レコーダ53が登録不可ではないと判定された場合、ステップS224に進み、レコーダ53のSAM66は、レシーバ51のSAM62に、内蔵する記憶モジュールに記憶している配送用鍵Kd（後述する図49のステップS235でレシーバ51から受け取っている）のバージョンおよび課金情報（後述する図54に対応する処理のステップS337に相当する処理で記憶している）を一時鍵Ktempで暗号化して、送信し、レシーバ51のSAM62は、配送用鍵Kdのバージョンおよび課金情報を受信し、復号する。

【0155】ステップS225において、レシーバ51の相互認証モジュール71は、通信部61を介して、EMDサービスセンタ1の相互認証部17と、相互認証する。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS226において、EMDサービスセンタ1のユーザ管理部18は、レシーバ51のIDを基に、ユーザ登録データベースを検索し、レシーバ51が登録不可であるか否かを判定し、レシーバ51が登録不可ではないと判定された場合、ステップS227に進み、レシーバ51のSAM62は、通信部61を介して、EMDサービスセンタ1のユーザ管理部18に、一時鍵Kdで暗号化した、記憶モジュール73に記憶している配送用鍵Kdのバージョン、課金情報、および登録リスト、HDD52に記録し

ている取扱方針、並びにレコーダ53の課金情報を送信する。ステップS228において、EMDサービスセンタ1のユーザ管理部18は、受信したデータを復号した後、課金情報を処理し、図42で説明した、レシーバ51から受信した登録リストのレコーダ53に関する登録拒絶フラグ、ステータスフラグなどのデータの部分を更新し、レシーバ51に対応するデータに応じた署名を付する。

【0156】ステップS229乃至ステップS234の処理は、図47に示すステップS186乃至ステップS191とそれぞれ同様であるので、その説明は省略する。

【0157】ステップS234において、レシーバ51のSAM62は、更新した登録リストを参照し、レコーダ53が登録不可か否かを判定し、レコーダ53が登録不可でないと判定された場合、ステップS235に進み、レコーダ53に、一時鍵Kdで暗号化した、課金情報受信メッセージ、および配送用鍵Kdを送信し、レコーダ53は、課金情報受信メッセージ、および配送用鍵Kdを受信し、復号する。ステップS236において、レコーダ53のSAM66は、内蔵する記憶モジュールに記憶している、課金情報を消去し、配送用鍵Kdを最新のバージョンに更新する。

【0158】ステップS222において、レシーバ51の記憶モジュール73に記憶する登録リストにレコーダ53のデータが載っていないと判定された場合、ステップS237に進み、図47に示したレコーダ53の登録処理を実行し、ステップS224に進む。

【0159】ステップS223において、レコーダ53が登録不可であると判定された場合、ステップS226において、レシーバ51が登録不可であると判定された場合、および、ステップS234において、レコーダ53が登録不可であると判定された場合、処理は終了する。

【0160】以上のように、レシーバ51に従属するレコーダ53は、レシーバ51を介して、配送用鍵Kdを受け取る。

【0161】次に、図34のステップS14に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を、図50のフローチャートを用いて説明する。ステップS251において、コンテンツプロバイダ2のウォータマーク付加部32は、コンテンツサーバ31から読み出したコンテンツに、コンテンツプロバイダ2を示す所定のウォータマークを挿入し、圧縮部33に供給する。ステップS252において、コンテンツプロバイダ2の圧縮部33は、ウォータマークが挿入されたコンテンツをATRAC2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS253において、乱数発生部35は、コンテンツ鍵Kcoとして用いる乱数を発生させ、暗号

化部 34 に供給する。ステップ S 254 において、コンテンツプロバイダ 2 の暗号化部 34 は、DES などの所定の方式で、コンテンツ鍵 Kc o を使用して、ウォーターマークが挿入され、圧縮されたコンテンツを暗号化する。

【0162】ステップ S 255 において、暗号化部 36 は、DES などの所定の方式で、図 34 のステップ S 11 の処理により、EMD サービスセンタ 1 から供給されている配送用鍵 K d でコンテンツ鍵 Kc o を暗号化する。ステップ S 256 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、およびポリシー記憶部 37 から供給された取扱方針にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 K s c p で暗号化し、図 13 に示すような署名を作成する。ステップ S 257 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、ポリシー記憶部 37 から供給される取扱方針、およびステップ S 256 で生成した署名を含んだ、図 13 に示すようなコンテンツプロバイダセキュアコンテナを作成する。

【0163】ステップ S 258 において、コンテンツプロバイダ 2 の相互認証部 39 は、サービスプロバイダ 3 の相互認証部 45 と相互認証する。この認証処理は、図 37 乃至図 39 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S 259 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、サービスプロバイダ 3 に、コンテンツプロバイダセキュアコンテナに、予め認証局から発行してもらった証明書を付して送信し、処理を終了する。

【0164】以上のように、コンテンツプロバイダ 2 は、サービスプロバイダ 3 に、コンテンツプロバイダセキュアコンテナを送信する。

【0165】コンテンツ鍵 Kc o と共に取扱方針を配送用鍵 K d で暗号化する例の場合の、コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する他の処理の詳細を、図 51 のフローチャートを用いて説明する。ステップ S 271 乃至ステップ S 274 の処理は、図 50 のステップ S 251 乃至ステップ S 254 の処理とそれぞれ同様であり、その説明は省略する。ステップ S 275 において、コンテンツプロバイダ 2 の暗号化部 36 は、図 35 のステップ S 21 の処理により、EMD サービスセンタ 1 から供給されている配送用鍵 K d を用いて、DES などの所定の方式で、コンテンツ鍵 Kc o およびポリシー記憶部 37 から供給される取扱方針を暗号化する。

【0166】ステップ S 276 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、および暗号化された取扱方針にハッシュ関数を適用しハッシュ値を算出し、自分自身の秘密鍵 K s c p で暗号化

し、図 25 に示すような署名を作成する。ステップ S 277 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、暗号化された取扱方針、および署名を含んだ、図 25 に示すようなコンテンツプロバイダセキュアコンテナを作成する。ステップ S 278 およびステップ S 279 の処理は、図 50 のステップ S 258 およびステップ S 259 の処理とそれぞれ同様であり、その説明は省略する。

10 【0167】このように、コンテンツプロバイダ 2 は、サービスプロバイダ 3 に、暗号化された取扱方針を含むコンテンツプロバイダセキュアコンテナを送信する。

【0168】次に、図 34 のステップ S 15 に対応する、サービスプロバイダ 3 がレシーバ 51 にサービスプロバイダセキュアコンテナを送信する処理の詳細を図 52 のフローチャートを用いて説明する。ステップ S 291 において、サービスプロバイダ 3 の値付け部 42 は、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、コンテンツプロバイダ 2 の公開鍵 K p c p を取り出す。証明書の署名の確認は、図 39 のステップ S 83 における処理と同様であるので、その説明は省略する。

【0169】ステップ S 292 において、サービスプロバイダ 3 の値付け部 42 は、コンテンツプロバイダ 2 のセキュアコンテナ作成部 38 から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ 2 の公開鍵 K p c p で復号し、得られたハッシュ値が、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、および取扱方針にハッシュ関数を適用し得られたハッシュ値と一致することを確認し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。改竄が発見された場合は、処理を終了する。

【0170】コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップ S 293 において、サービスプロバイダ 3 の値付け部 42 は、コンテンツプロバイダセキュアコンテナから取扱方針を取り出す。ステップ S 294 において、サービスプロバイダ 3 の値付け部 42 は、取扱方針を基に、図 17 で説明した価格情報を作成する。ステップ S 295 において、サービスプロバイダ 3 のセキュアコンテナ作成部 44 は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、取扱方針、価格情報、並びに暗号化されたコンテンツ、暗号化されたコンテンツ鍵 Kc o、取扱方針、および価格情報にハッシュ関数を適用して得られたハッシュ値を、自分自身の秘密鍵 K s s p で暗号化し、得られた値を署名として図 15 に示すようなサービスプロバイダセキュアコンテナを作成する。

【0171】ステップ S 296 において、サービスプロ

バイダ3の相互認証部45は、レシーバ51の相互認証モジュール71と相互認証する。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS297において、サービスプロバイダ3のセキュアコンテナ作成部44は、レシーバ51の通信部61に、証明書を付したサービスプロバイダセキュアコンテナを送信し、処理を終了する。

【0172】このように、サービスプロバイダ3は、レシーバ51にサービスプロバイダセキュアコンテナを送信する。

【0173】コンテンツプロバイダ2において、取扱方針が配送用鍵Kdで暗号化され、かつ、サービスプロバイダ3が取扱制御情報を作成する例の場合の、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理の詳細を、図53のフローチャートを用いて説明する。ステップS311およびステップS312の処理は、図52のステップS291およびステップS292の処理とそれぞれ同様であるので、その説明は省略する。ステップS313において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナに含まれる暗号化された取扱方針を復号する。ステップS314において、サービスプロバイダ3の値付け部42は、取扱方針を基に、図23で説明した取扱制御情報を作成する。ステップS315乃至ステップS318の処理は、図52のステップS294およびステップS297の処理とそれぞれ同様であるので、その説明は省略する。

【0174】このように、サービスプロバイダ3は、レシーバ51に暗号化された取扱方針を含むサービスプロバイダセキュアコンテナを送信する。

【0175】図34のステップS16に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、レシーバ51の課金処理の詳細を、図54のフローチャートを用いて説明する。ステップS331において、レシーバ51の復号/暗号化モジュール74は、配送用鍵Kdでコンテンツ鍵Kcを復号できるか否かを判定し、配送用鍵Kdでコンテンツ鍵Kcを復号できないと判定された場合、ステップS332で、レシーバ51は、図48で説明した配送用鍵Kdの受け取り処理を実行し、ステップS333に進む。ステップS331において、配送用鍵Kdでコンテンツ鍵Kcを復号できると判定された場合、手続は、ステップS332をスキップし、ステップS333に進む。ステップS333において、レシーバ51の復号ユニット91は、図34のステップS13の処理により、記憶モジュール73に記憶されている配送用鍵Kdで、コンテンツ鍵Kcを復号する。

【0176】ステップS334において、レシーバ51の課金処理モジュール72は、サービスプロバイダセキ

ュアコンテナに含まれる取扱方針および価格情報を取り出し、図19および図20で説明した課金情報および使用許諾条件情報を生成する。ステップS335において、レシーバ51の課金処理モジュール72は、記憶モジュール73に記憶している課金情報およびステップS334で算出された課金情報から、現在の課金が課金の上限以上であるか否かを判定し、現在の課金が課金の上限以上であると判定された場合、ステップS336に進み、レシーバ51は図48で説明した配送用鍵Kdの受け取り処理を実行し、新たな配送用鍵Kdを受け取り、ステップS337に進む。ステップS335において、現在の課金が課金の上限未満であると判定された場合、ステップS336はスキップされ、ステップS337に進む。

【0177】ステップS337において、レシーバ51の課金処理モジュール72は、記憶モジュール73に課金情報を記憶させる。ステップS338において、レシーバ51の課金処理モジュール72は、ステップS334にて生成した使用許諾条件情報をHDD52に記録する。ステップS339において、レシーバ51のSAM62は、HDD52にサービスプロバイダセキュアコンテナから取り出した取扱方針を記録させる。

【0178】ステップS340において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS341において、レシーバ51の記憶モジュール73は、使用許諾条件情報のハッシュ値を記憶する。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS342において、レシーバ51の乱数発生ユニット92は、保存用鍵Ksaveである乱数を発生し、ステップS343に進む。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS342はスキップされ、ステップS343に進む。

【0179】ステップS343において、レシーバ51の暗号化ユニット93は、コンテンツ鍵Kcを保存用鍵Ksaveで暗号化する。ステップS344において、レシーバ51のSAM62は、暗号化されたコンテンツ鍵KcをHDD52に記憶させる。記憶モジュール73に保存用鍵Ksaveが記憶されていない場合、ステップS345において、レシーバ51の復号/暗号化モジュール74は、保存用鍵Ksaveを記憶モジュール73に記憶させ、処理は終了する。記憶モジュール73に保存用鍵Ksaveが記憶されている場合、ステップS345はスキップされ、処理は終了する。

【0180】以上のように、レシーバ51は、課金情報を記憶モジュール73に記憶すると共に、コンテンツ鍵Kcを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、記憶モジュール73に記憶される。

【0181】レコーダ53も、同様の処理で、課金情報をSAM66内の記憶モジュールに記憶すると共に、コンテンツ鍵Kcoを配送用鍵Kdで復号し、再度、コンテンツ鍵Kcoを保存用鍵Ksaveで暗号化し、HDD52に記録させる。保存用鍵Ksaveは、SAM66内の記憶モジュールに記憶される。

【0182】図34のステップS17に対応するレシーバ51がコンテンツを再生する処理の詳細を、図55のフローチャートを用いて説明する。ステップS361において、レシーバ51の復号/暗号化モジュール74は、HDD52から、図54のステップS338で記憶した使用許諾条件情報およびステップS344で記憶した暗号化されたコンテンツ鍵Kcoを読み出す。ステップS362において、レシーバ51の復号/暗号化モジュール74は、使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。

【0183】ステップS363において、レシーバ51の復号/暗号化モジュール74は、ステップS362において算出されたハッシュ値が、図54のステップS340で記憶モジュール73に記憶されたハッシュ値と一致するか否かを判定し、ステップS362において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値と一致すると判定された場合、ステップS364に進み、使用回数の値などの使用許諾条件情報に含まれる所定の情報を更新する。ステップS365において、レシーバ51の復号/暗号化モジュール74は、更新した使用許諾条件情報にハッシュ関数を適用しハッシュ値を算出する。ステップS366において、レシーバ51の記憶モジュール73は、ステップS365で算出した使用許諾条件情報のハッシュ値を記憶する。ステップS367において、レシーバ51の復号/暗号化モジュール74は、HDD52に更新した使用許諾条件情報を記録させる。

【0184】ステップS368において、SAM62の相互認証モジュール71と伸張部63の相互認証モジュール75は、相互認証し、SAM62および伸張部63は、一時鍵Ktempを記憶する。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、またはR3が、一時鍵Ktempとして用いられる。ステップS369において、復号/暗号化モジュール74の復号ユニット91は、図54のステップS344にてHDD52に記録されたコンテンツ鍵Kcoを、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。ステップS370において、復号/暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵Kcoを一時鍵Ktempで暗号化する。ステップS371において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを伸張部63に送信する。

【0185】ステップS372において、伸張部63の復号モジュール76は、コンテンツ鍵Kcoを一時鍵Ktempで復号する。ステップS373において、SAM62は、HDD52に記録されたコンテンツを読み出し、伸張部63に送信する。ステップS374において、伸張部63の復号モジュール77は、コンテンツをコンテンツ鍵Kcoで復号する。ステップS375において、伸張部63の伸張モジュール78は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS376において、伸張部63のウォーターマーク付加モジュール79は、伸張されたコンテンツにレシーバ51を特定する所定のウォーターマークを挿入する。ステップS377において、レシーバ51は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0186】ステップS363において、ステップS362において算出されたハッシュ値が、記憶モジュール73に記憶されたハッシュ値と一致しないと判定された場合、ステップS378において、SAM62は、図示せぬ表示装置にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0187】このように、レシーバ51は、コンテンツを再生する。

【0188】図56は、図11の構成を有するユーザホームネットワーク5において、レシーバ51がデコーダ56にコンテンツを再生させる処理を説明するフローチャートである。ステップS391乃至ステップS397の処理は、図55のステップS361乃至ステップS367の処理とそれぞれ同様であるので、その説明は省略する。

【0189】ステップS398において、SAM62の相互認証モジュール71とデコーダ56の相互認証モジュール101は、相互認証し、一時鍵Ktempが共有される。この認証処理は、図37乃至図39を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、またはR3が、一時鍵Ktempとして用いられる。ステップS399において、復号/暗号化モジュール74の復号ユニット91は、HDD52に記録されたコンテンツ鍵Kcoを、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。ステップS400において、復号/暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵Kcoを一時鍵Ktempで暗号化する。ステップS401において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoをデコーダ56に送信する。

【0190】ステップS402において、デコーダ56の復号モジュール102は、コンテンツ鍵Kcoを一時鍵Ktempで復号する。ステップS403において、SAM62は、HDD52に記録されたコンテンツを読み出し、デコーダ56に送信する。ステップS404におい

て、デコーダ56の復号モジュール103は、コンテンツをコンテンツ鍵Kcで復号する。ステップS405において、デコーダ56の伸張モジュール104は、復号されたコンテンツをATRAC2などの所定の方式で伸張する。ステップS406において、デコーダ56のウォータマーク付加モジュール105は、伸張されたコンテンツにデコーダ56を特定する所定のウォータマークを挿入する。ステップS407において、デコーダ56は、図示せぬスピーカなどに再生されたコンテンツを出力し、処理を終了する。

【0191】ステップS408の処理は、図55のステップS378の処理と同様であるので、その説明は省略する。

【0192】以上のように、ユーザホームネットワークが図11に示す構成を有する場合、レシーバ51が受信したコンテンツは、デコーダ56で再生される。

【0193】図61を参照して後述する決済処理の前に行われる、EMDサービスセンタ1の決済オブジェクトを作成する処理を、図57のフローチャートを参照して説明する。ステップS421において、EMDサービスセンタ1の経歴データ管理部15は、図47のステップS187またはステップS189などでユーザホームネットワーク5から受信し、記憶した課金情報の中から、所定のコンテンツの利用に関する課金情報を選択し、選択した課金情報を利益分配部16に送信する。ステップS422において、利益分配部16は、経歴データ管理部15から受信した課金情報にコンテンツプロバイダ2およびサービスプロバイダ3への利益配分を示すデータが含まれているか否かを判定し、経歴データ管理部15から受信した課金情報にコンテンツプロバイダ2およびサービスプロバイダ3への利益配分を示すデータが含まれていると判定された場合、ステップS423に進む。

【0194】ステップS423において、利益分配部16は、課金情報に含まれる利益配分を示すデータを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ3への支払い額を算出する。ステップS424において、利益分配部16は、課金情報に含まれる利益配分を示すデータを参照して、サービスプロバイダ3からコンテンツプロバイダ2への支払い額を算出する。ステップS425において、利益分配部16は、課金情報に含まれる利益配分を示すデータを参照して、コンテンツプロバイダ2から権利団体への支払い額を算出し、ステップS429に進む。

【0195】ステップS422において、経歴データ管理部15から受信した課金情報にコンテンツプロバイダ2およびサービスプロバイダ3への利益配分を示すデータが含まれていないと判定された場合、ステップS426に進み、利益分配部16は、利益分配部16が記憶する利益配分データベースを参照して、所定のコンテンツを利用したユーザからサービスプロバイダ3への支払い

額を算出する。ステップS427において、利益分配部16は、利益分配部16が記憶する利益配分データベースを参照して、サービスプロバイダ3からコンテンツプロバイダ2への支払い額を算出する。ステップS428において、利益分配部16は、利益分配部16が記憶する利益配分データベースを参照して、コンテンツプロバイダ2から権利団体への支払い額を算出し、ステップS429に進む。

【0196】ステップS429において、利益分配部16は、利益分配部16に記憶されている割引情報データベースのデータを参照して、所定のユーザからサービスプロバイダ3への支払い額、サービスプロバイダ3からコンテンツプロバイダ2への支払い額、およびコンテンツプロバイダ2から権利団体への支払額を補正する。

【0197】ステップS430において、経歴データ管理部15は、すべてのコンテンツについてステップS423乃至ステップS429の計算を実行したか否かを判定し、すべてのコンテンツについてステップS423乃至ステップS429の計算をまだ実行していないと判定された場合、手続きは、ステップS421に戻り、それ以降の処理を繰り返す。ステップS430において、すべてのコンテンツについてステップS421乃至ステップS429の計算が実行されたと判定された場合、手続きは、ステップS431に進む。

【0198】ステップS431において、利益分配部16は、ユーザ毎に各サービスプロバイダ3への支払金額を算出し、クレジット決済オブジェクト1（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図58（A）に示すクレジット決済オブジェクト

1）を作成する。クレジット決済オブジェクト1では、支払元にユーザのIDが設定され、支払先にサービスプロバイダ3のIDが設定され、支払額にサービスプロバイダ3への支払額が設定される。ステップS432において、利益分配部16は、サービスプロバイダ3毎に各コンテンツプロバイダ2への支払金額を算出し、クレジット決済オブジェクト2（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図58（B）に示すクレジット決済オブジェクト2）を作成する。クレジット決済オブジェクト2では、支払元にクレジット決済オブジェクト1が設定され、支払先にコンテンツプロバイダ2のIDが設定され、支払額にコンテンツプロバイダ2への支払額が設定される。

【0199】ステップS433において、利益分配部16は、コンテンツプロバイダ2毎に権利団体への支払金額を算出し、クレジット決済オブジェクト3（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図58（C）に示すクレジット決済オブジェクト3）を作成する。クレジット決済オブジェクト3では、支払元にクレジット決済オブジェクト1が設定され、支払先に権利団体のIDが設定され、支払額に権利団体への

支払額が設定される。ステップS434において、課金請求部19は、課金請求部19が記憶する、ユーザに対するEMDサービスセンタ1の利用料金を格納するユーザ利用料金テーブルを参照してユーザからの徴収金額を算出し、クレジット決済オブジェクト4（例えば、ユーザがクレジットカードを使用して利用料金を支払う場合、図58（D）に示すクレジット決済オブジェクト4）を作成し、クレジット決済オブジェクト1の徴収額を設定し、処理を終了する。クレジット決済オブジェクト4では、支払元にクレジット決済オブジェクト1が設定され、支払先にEMDサービスセンタ1のIDが設定され、支払額にEMDサービスセンタ1への支払額が設定される。

【0200】以上のように、EMDサービスセンタ1は、決済オブジェクトを作成する。

【0201】図59は、サービスプロバイダ3、コンテンツプロバイダ2、および権利団体が、EMDサービスセンタ1にサービス料を銀行決済で支払う場合の、銀行決済オブジェクトの例を示す図である。図59（A）の銀行決済オブジェクト1では、支払元にサービスプロバイダ3のIDが設定され、徴収額にサービスプロバイダ3からの徴収額が設定され、支払先にEMDサービスセンタ1のIDが設定され、支払額にEMDサービスセンタ1への支払額（徴収額と同額）が設定される。図59（B）の銀行決済オブジェクト2では、支払元にコンテンツプロバイダ2のIDが設定され、徴収額にコンテンツプロバイダ2からの徴収額が設定され、支払先にEMDサービスセンタ1のIDが設定され、支払額にEMDサービスセンタ1への支払額（徴収額と同額）が設定される。図59（C）の銀行決済オブジェクト3では、支払元に権利団体のIDが設定され、徴収額に権利団体からの徴収額が設定され、支払先にEMDサービスセンタ1のIDが設定され、支払額にEMDサービスセンタ1への支払額（徴収額と同額）が設定される。

【0202】図60は、ユーザがクレジットカードを利用して料金を支払い、サービスプロバイダ3、およびコンテンツプロバイダ2は銀行口座を利用して決済を行う場合の、決済オブジェクトの例を示す図である。図60

（A）および図60（D）のクレジット決済オブジェクトは、図58（A）および図58（D）のクレジット決済オブジェクトとそれぞれ同様であり、その説明は省略する。図60（B）の銀行決済オブジェクト2は、支払元にサービスプロバイダ3のIDが設定され、徴収額に、コンテンツプロバイダ2への支払額と権利団体への支払額を合わせた、サービスプロバイダ3からの金額が設定され、支払先にコンテンツプロバイダ2のIDが設定され、支払額にコンテンツプロバイダ2への支払額（徴収額と同額）が設定される。図60（C）の銀行決済オブジェクト3は、支払元にコンテンツプロバイダ2のIDが設定され、徴収額に、コンテンツプロバイダ2からの徴収額が設定され、支払先に権利団体のIDが設定され、支

払額に権利団体への支払額（徴収額と同額）が設定される。

【0203】図58、図59、および図60の決済オブジェクトに記述された、支払先、徴収額、支払先、および支払額に基づき、決済が実行されことにより、EMDサービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、および権利団体に所定の金額が支払われる。EMDサービスセンタ1のクレジット決済処理オブジェクトを用いる決済の処理を図61のフローチャートを参照して説明する。ステップS451において、EMDサービスセンタ1の出納部20は、クレジット決済オブジェクトの支払先に記載されているIDより、支払先の銀行などの決済機関を求める。ステップS452において、EMDサービスセンタ1の出納部20は、クレジット決済オブジェクトの支払元に記載されているIDより、支払元のクレジット会社などの決済機関を求める。ステップS453において、出納部20は、予め記憶された情報により、支払元の与信処理が必要であるか否かを判定し、支払元の与信処理が必要であると判定された場合、ステップS454において、与信処理を実行する。ステップS454の与信処理において、支払元が支払いできないと判定された場合、処理は終了する。ステップS454の与信処理において、支払元が支払いできると判定された場合、ステップS455に進む。

【0204】ステップS453において、支払元の与信処理が必要でないと判定された場合、手続きは、ステップS454をスキップし、ステップS455に進む。

【0205】ステップS455において、出納部20は、前に実行された決済オブジェクトの処理が完了しているか否かを判定し、前に実行された決済オブジェクトの処理が完了していると判定された場合、ステップS456に進み、ステップS451およびステップS452で求めた決済機関に、クレジット決済オブジェクトに記載された徴収額、および支払い額に対応した決済命令を送信する。ステップS457において、クレジット決済オブジェクトの支払先に記載されているIDに対応する支払い先にステップS456で実行した決済処理の情報を送信する。ステップS458において、クレジット決済オブジェクトの支払元に記載されているIDに対応する支払い元にステップS456で実行した決済処理の情報を送信し、処理は終了する。

【0206】ステップS455において、前に実行された決済オブジェクトの処理が完了していないと判定された場合、ステップS459に進み、出納部20は、処理が完了していない決済オブジェクトに記載された支払い元に所定のメッセージを送信する等の、決済未完了の所定のエラー処理を実行し、処理は終了する。

【0207】以上のように、クレジット決済処理オブジェクトを用いる決済が処理される。

【0208】図62は、EMDサービスセンタ1の銀行決

済処理オブジェクトを用いる決済の処理を説明するフローチャートである。銀行決済処理オブジェクトを用いる決済の処理は、図 61 に示すクレジット決済処理オブジェクトを用いる決済の処理から、ステップ S 451 およびステップ S 454 の与信に関する処理を除いたものと同様である。ステップ S 471 およびステップ S 472 の処理は、図 61 のステップ S 451 およびステップ S 452 の処理とそれぞれ同様であるので、その説明は省略する。ステップ S 473 乃至ステップ S 477 の処理は、図 61 のステップ S 455 乃至ステップ S 459 の処理とそれぞれ同様であるので、その説明は省略する。

【0209】このように、銀行決済処理オブジェクトを用いる決済が処理され、クレジット決済処理オブジェクトを用いる決済の処理とともに、ユーザ、コンテンツプロバイダ 2、サービスプロバイダ 3、および権利団体から所定の金額が徴収され、EMD サービスセンタ 1、コンテンツプロバイダ 2、サービスプロバイダ 3、および権利団体に所定の金額が入金される。

【0210】なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であれば MPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0211】また、共通鍵暗号は、ブロック暗号である DES を使用して説明したが、NTT (商標) が提案する FEAL、IDEA (International Data Encryption Algorithm)、または 1 ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0212】さらに、コンテンツおよびコンテンツ鍵 K_{cc} の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0213】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0214】また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0215】

【発明の効果】請求項 1 に記載の情報処理装置、請求項 6 に記載の情報処理方法、および請求項 7 に記載の提供媒体によれば、情報を特定するデータおよび情報の利用に対する情報提供者の支払い金額を示すデータを記憶し、記憶するデータを基に、情報提供者毎の支払い金額の合計を算出し、情報提供者毎の利益を基に、決済機関に対し情報提供者毎の決済を指示するようにした

ので、精算処理および利益の算出の処理が効率良く出来るようになる。

【図面の簡単な説明】

【図 1】 EMD のシステムを説明する図である。

【図 2】 EMD サービスセンタ 1 の機能の構成を示すブロック図である。

【図 3】 EMD サービスセンタ 1 の配送用鍵 K_d の送信を説明する図である。

【図 4】 EMD サービスセンタ 1 の配送用鍵 K_d の送信を説明する図である。

【図 5】 EMD サービスセンタ 1 の配送用鍵 K_d の送信を説明する図である。

【図 6】 EMD サービスセンタ 1 の配送用鍵 K_d の送信を説明する図である。

【図 7】 ユーザ登録データベースを説明する図である。

【図 8】 コンテンツプロバイダ 2 の機能の構成を示すブロック図である。

【図 9】 サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 10】 ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 11】 ユーザホームネットワーク 5 の構成を示すブロック図である。

【図 12】 コンテンツおよびコンテンツに付随する情報を説明する図である。

【図 13】 コンテンツプロバイダセキュアコンテナを説明する図である。

【図 14】 コンテンツプロバイダ 2 の証明書を説明する図である。

【図 15】 サービスプロバイダセキュアコンテナを説明する図である。

【図 16】 サービスプロバイダ 3 の証明書を説明する図である。

【図 17】 取扱方針、価格情報、および使用許諾条件情報を示す図である。

【図 18】 シングルコピーおよびマルチコピーを説明する図である。

【図 19】 取扱方針および価格情報を説明する図である。

【図 20】 取扱方針、価格情報、および使用許諾条件情報を説明する図である。

【図 21】 コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 22】 サービスプロバイダセキュアコンテナを説明する図である。

【図 23】 取扱方針、取扱い制御情報、価格情報、及び使用許諾条件の構成を示す図である。

【図 24】 コンテンツおよびコンテンツに付随する情報の他の構成を説明する図である。

【図 25】 コンテンツプロバイダセキュアコンテナを説

明する図である。

【図 26】サービスプロバイダセキュアコンテナを説明する図である。

【図 27】EMDサービスセンタ 1 が、決算処理に必要なデータを収集する動作を説明する図である。

【図 28】利益配分データベースの例を示す図である。

【図 29】割引テーブルの例を示す図である。

【図 30】ユーザ利用料金テーブルの例を示す図である。

【図 31】EMDサービスセンタ 1 の、ユーザホームネットワーク 5 からの課金情報の受信のときの動作を説明する図である。

【図 32】EMDサービスセンタ 1 の利益配分処理の動作を説明する図である。

【図 33】EMDサービスセンタ 1 の、コンテンツの利用実績の情報を JASRAC に送信する処理の動作を説明する図である。

【図 34】コンテンツの配布の処理を説明するフローチャートである。

【図 35】コンテンツの配布の処理を説明するフローチャートである。

【図 36】EMDサービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 37】コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 38】コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 39】コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 40】レシーバ 5 1 の EMD サービスセンタ 1 への登録の処理を説明するフローチャートである。

【図 41】SAM の証明書を説明する図である。

【図 42】登録リストを説明する図である。

【図 43】IC カード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 44】IC カード 5 5 への SAM 6 2 のデータのバックアップの処理を説明するフローチャートである。

【図 45】新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 46】新しいレシーバに IC カード 5 5 のバックアップデータを読み込ませる処理を説明するフローチャートである。

【図 47】レシーバ 5 1 が、従属関係のあるレコーダ 5 3 を EMD サービスセンタ 1 に登録する処理を説明するフローチャートである。

【図 48】レシーバ 5 1 が EMD サービスセンタ 1 から配送用鍵 K d を受け取る処理を説明するフローチャートである。

【図 49】レコーダの配送用鍵 K d の受け取り処理を説明するフローチャートである。

【図 50】コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 51】コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する他の処理を説明するフローチャートである。

【図 52】サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 53】サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 54】レシーバ 5 1 の課金処理を説明するフローチャートである。

【図 55】レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

【図 56】レシーバ 5 1 がデコーダ 5 6 にコンテンツを再生させる処理を説明するフローチャートである。

【図 57】EMD サービスセンタ 1 の決済オブジェクトを作成する処理を説明するフローチャートである。

【図 58】クレジット決済オブジェクトの例を説明する図である。

【図 59】銀行決済オブジェクトの例を説明する図である。

【図 60】クレジット決済オブジェクトの例および銀行決済オブジェクトの例を説明する図である。

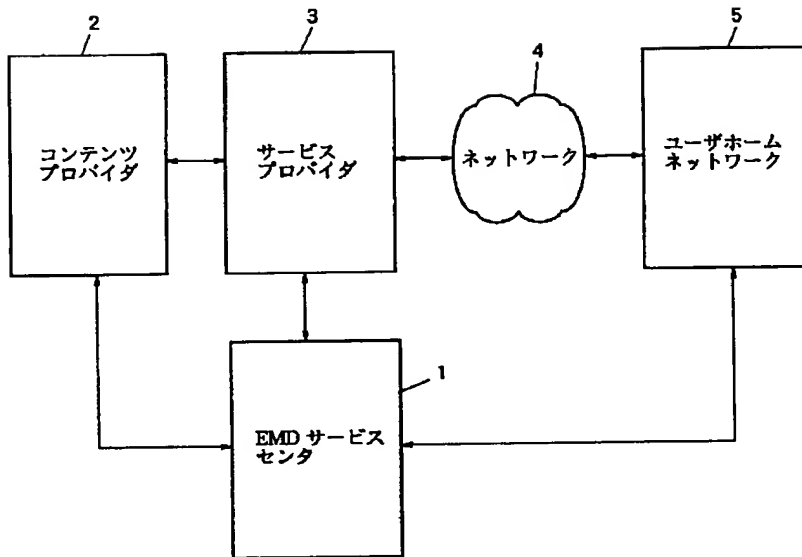
【図 61】クレジット決済処理を説明するフローチャートである。

【図 62】銀行決済処理を説明するフローチャートである。

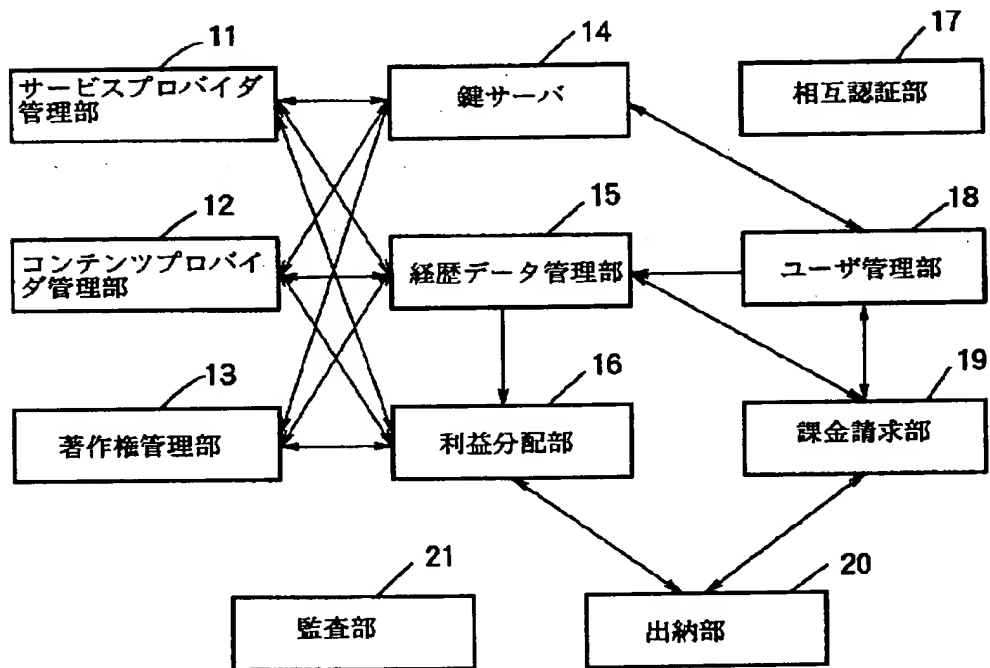
【符号の説明】

1 EMD サービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 15 経歴データ管理部, 16 利益配分部, 18 ユーザ管理部, 20 出納部, 42 値付け部, 51 レシーバ, 56 デコーダ, 61 通信部, 62 SAM, 63 伸張部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 相互認証モジュール, 76 復号モジュール, 77 復号モジュール, 81 相互認証モジュール, 91 復号ユニット, 92 暗号化ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール

【図 1】

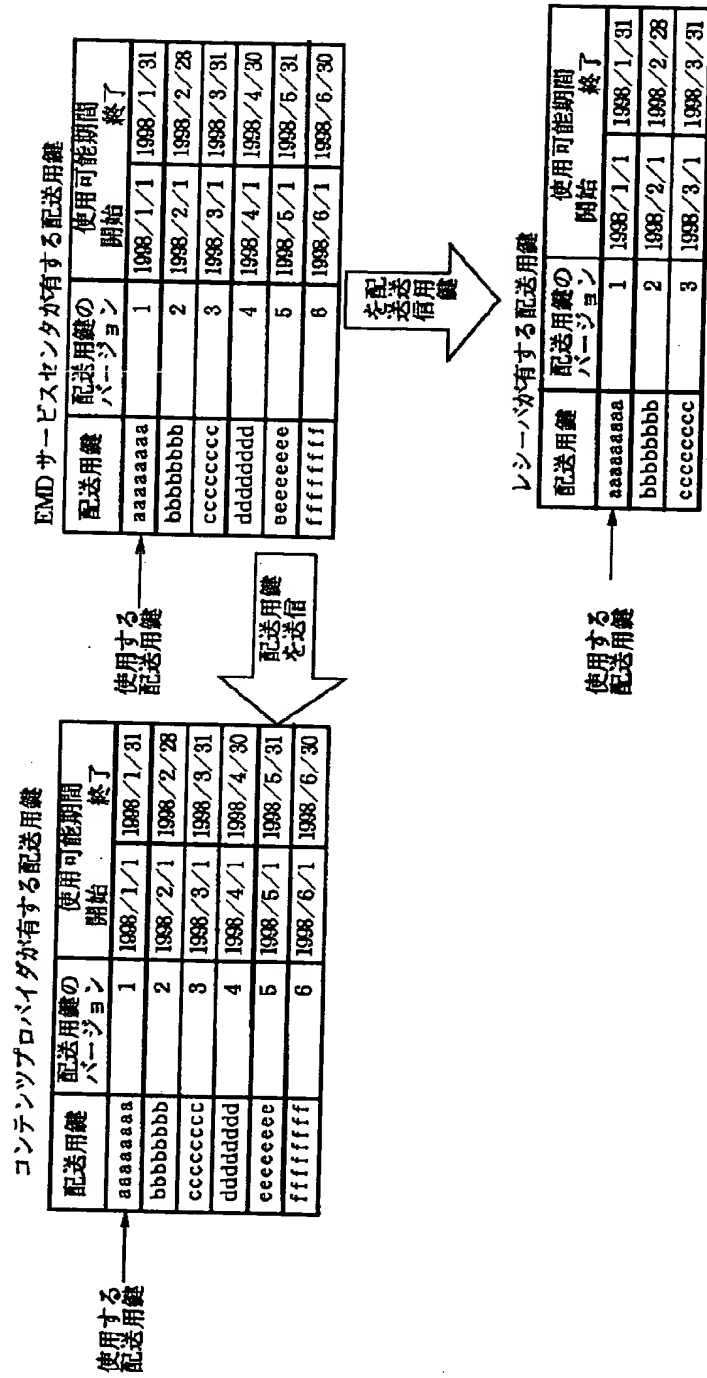


【図 2】

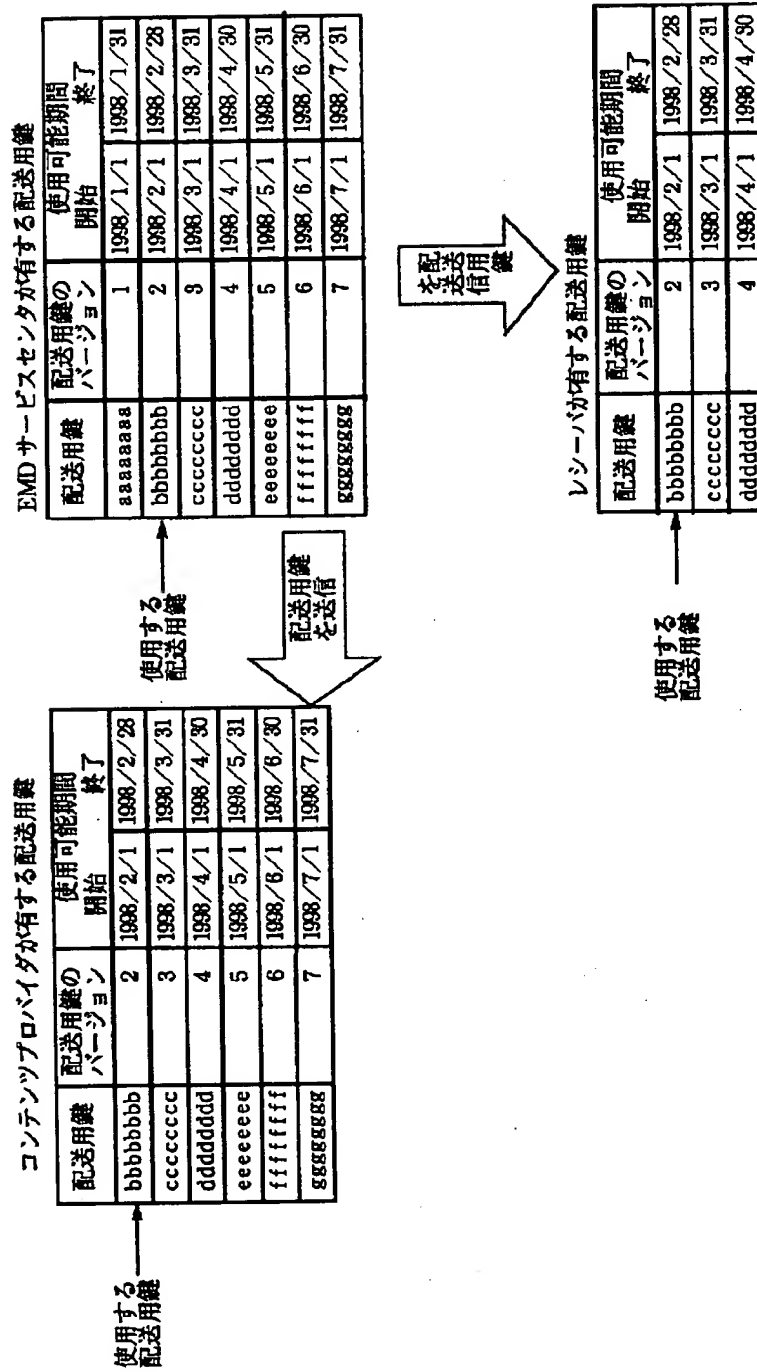


EMD サービスセンタ 1

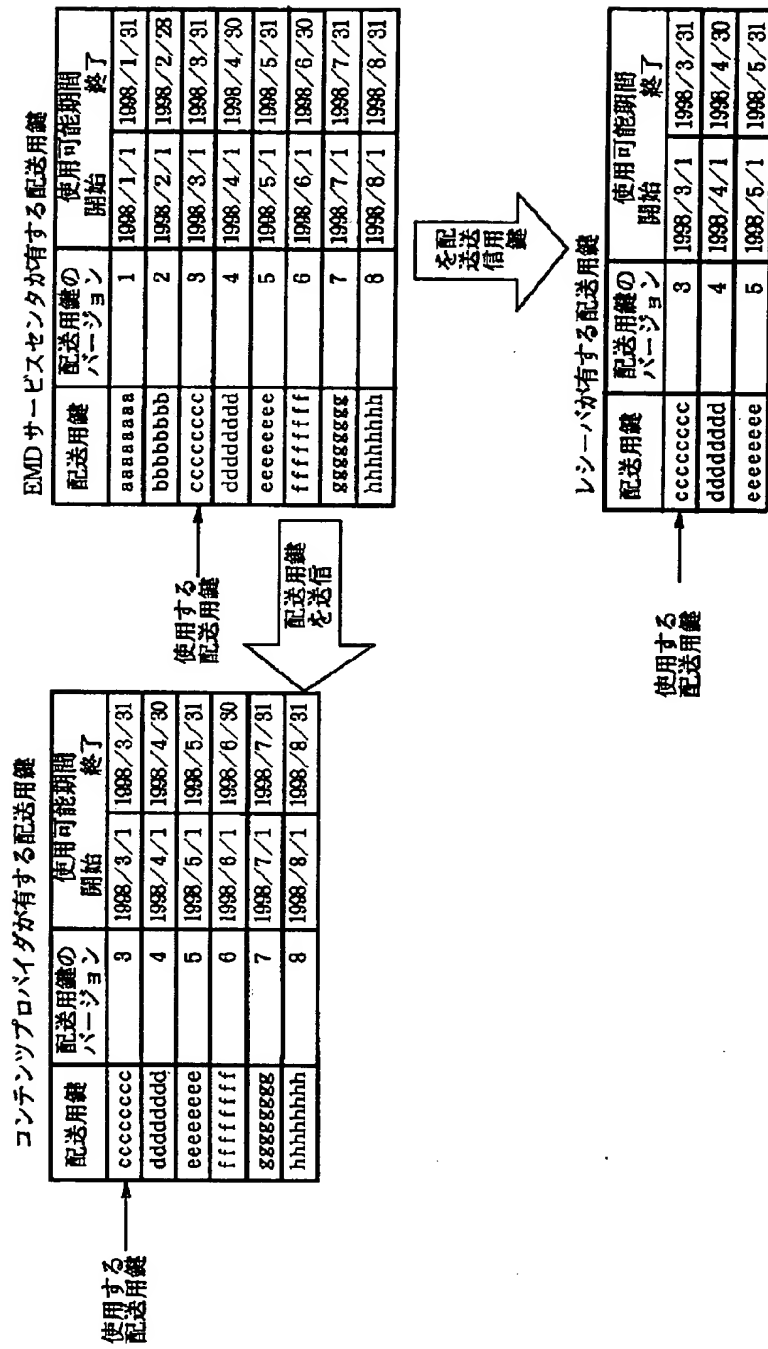
【図3】



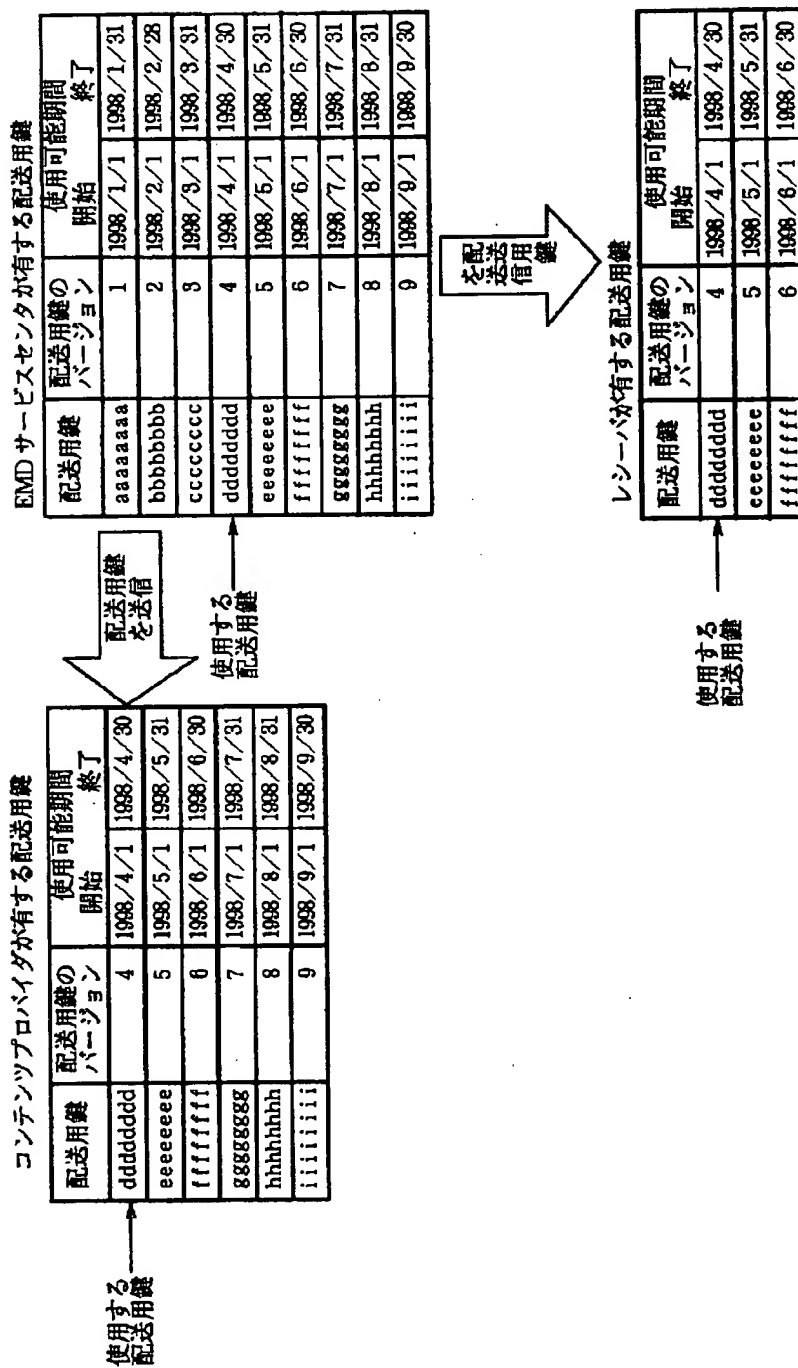
【図4】



【図 5】



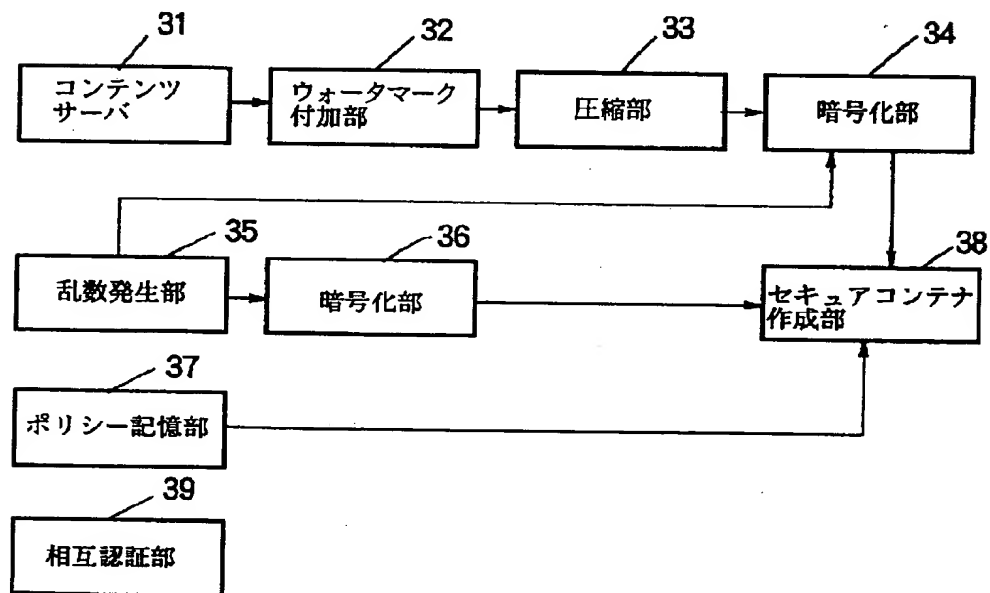
【図 6】



【図 7】

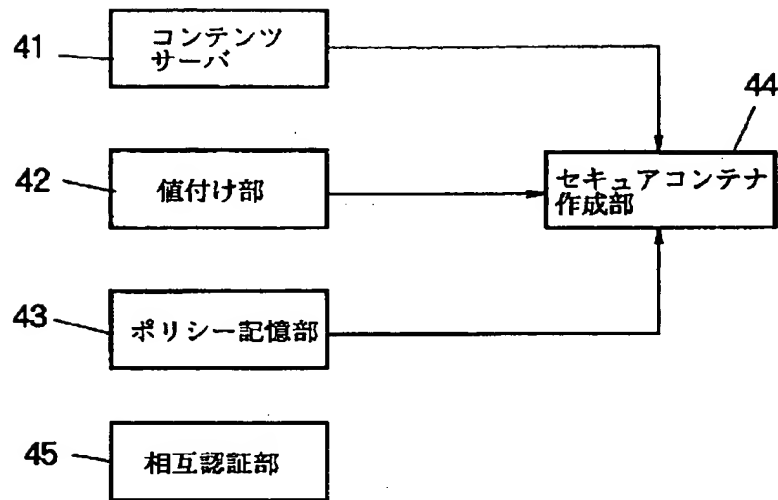
ID	決済処理	登録	EMD サービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
...			
FFFFFFFFFFFFFFFeh	可	不可	不可
FFFFFFFFFFFFFFFfh	不可	可	可

【図 8】



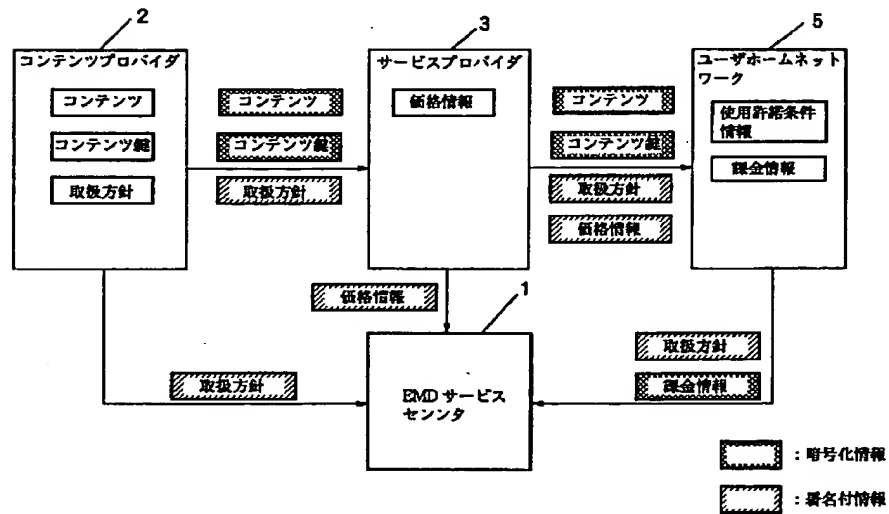
コンテンツプロバイダ 2

【図 9】



サービスプロバイダ 3

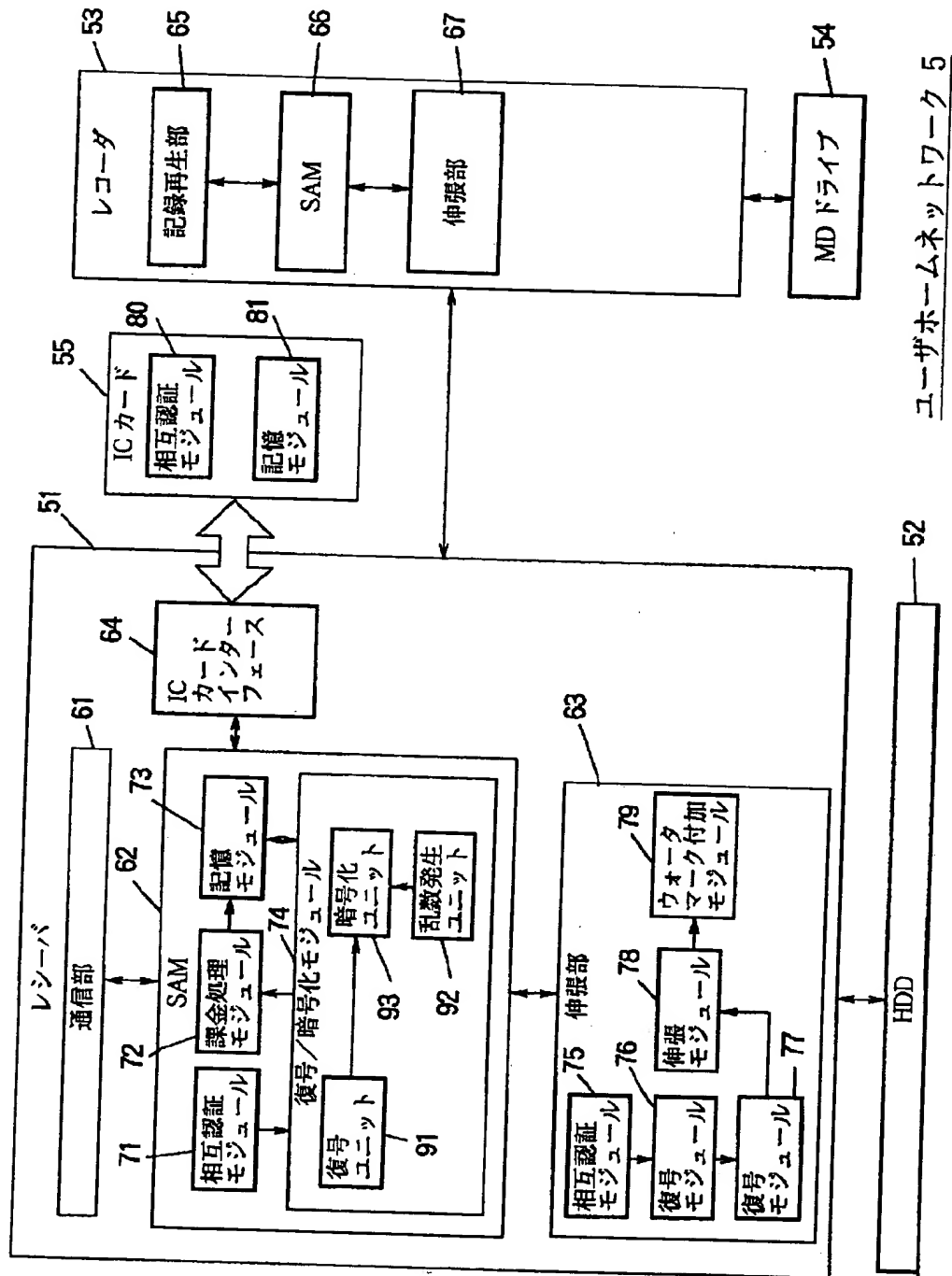
【図 12】



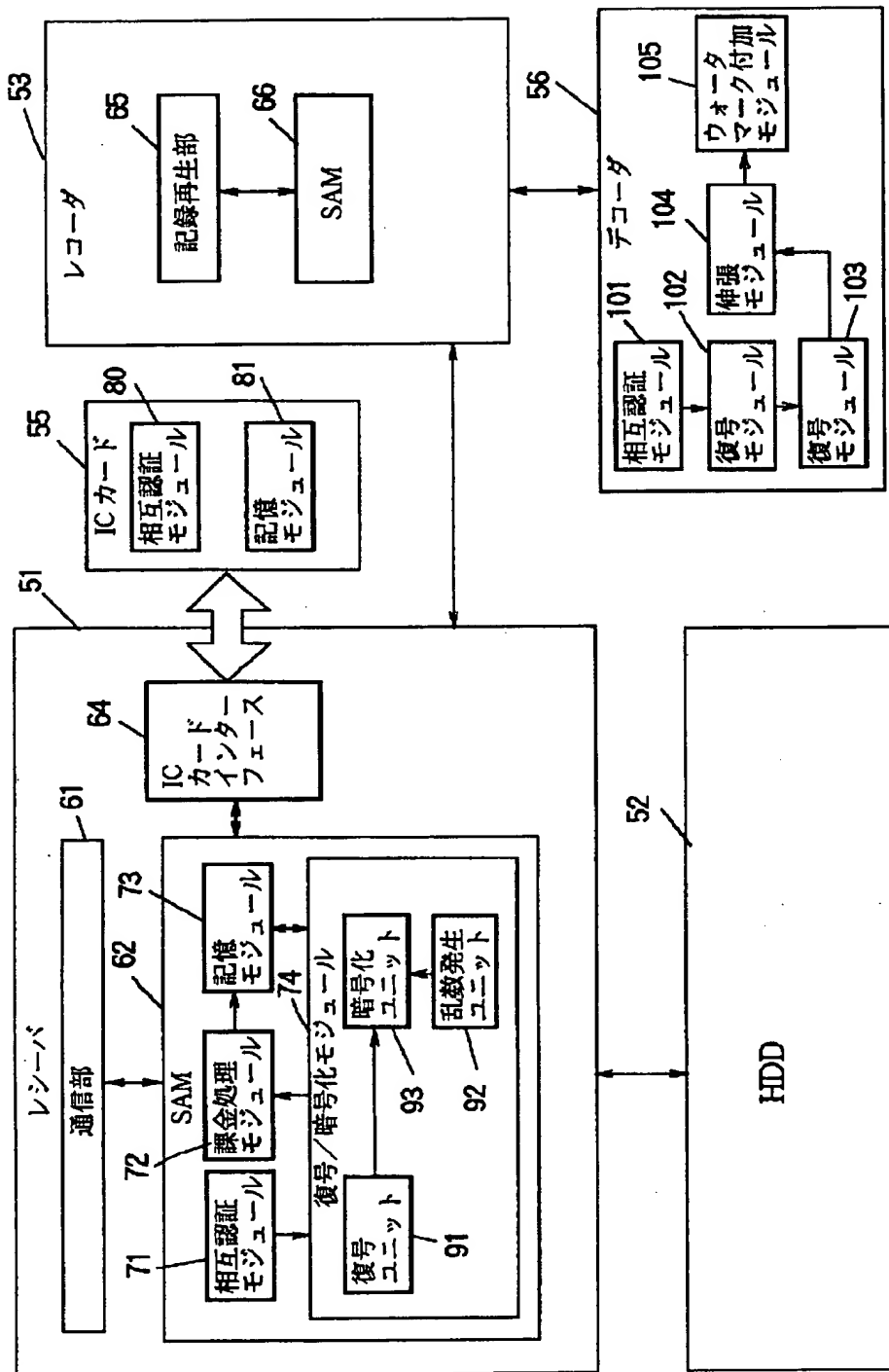
【図 28】

コンテンツ ID	コンテンツプロバイダ ID	権利団体
1	201	10%
2	201	20%

【図10】

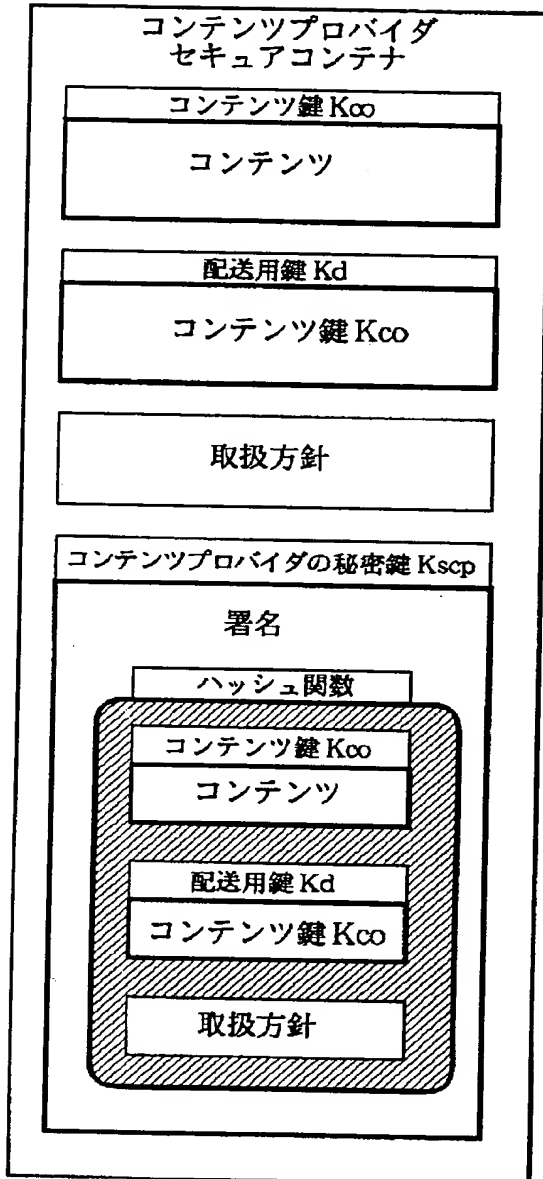


【図 11】

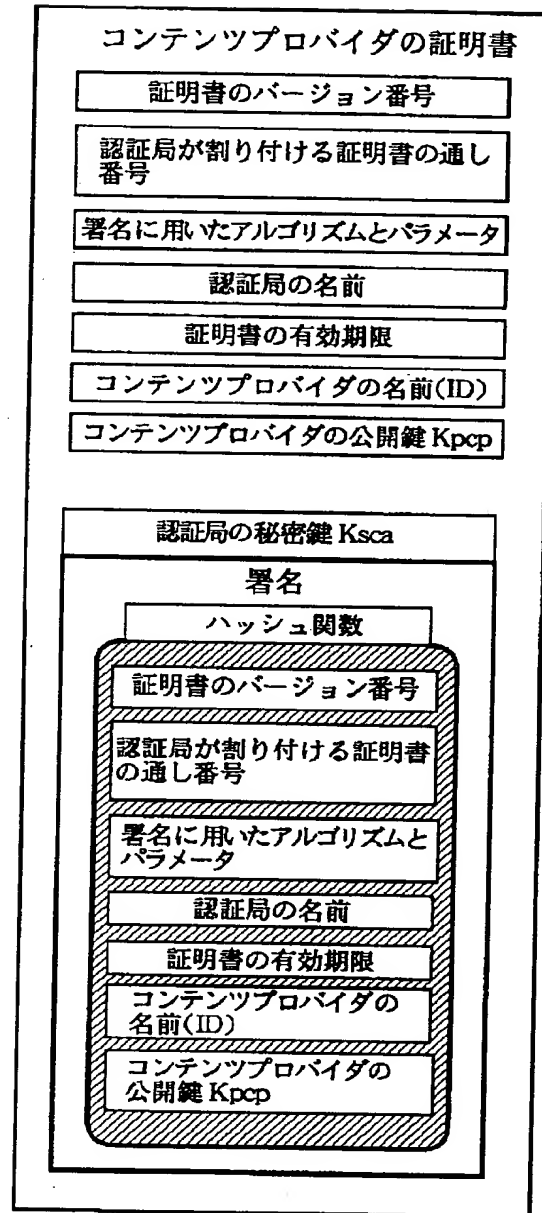


ユーザホームネットワーク 5

【図 13】



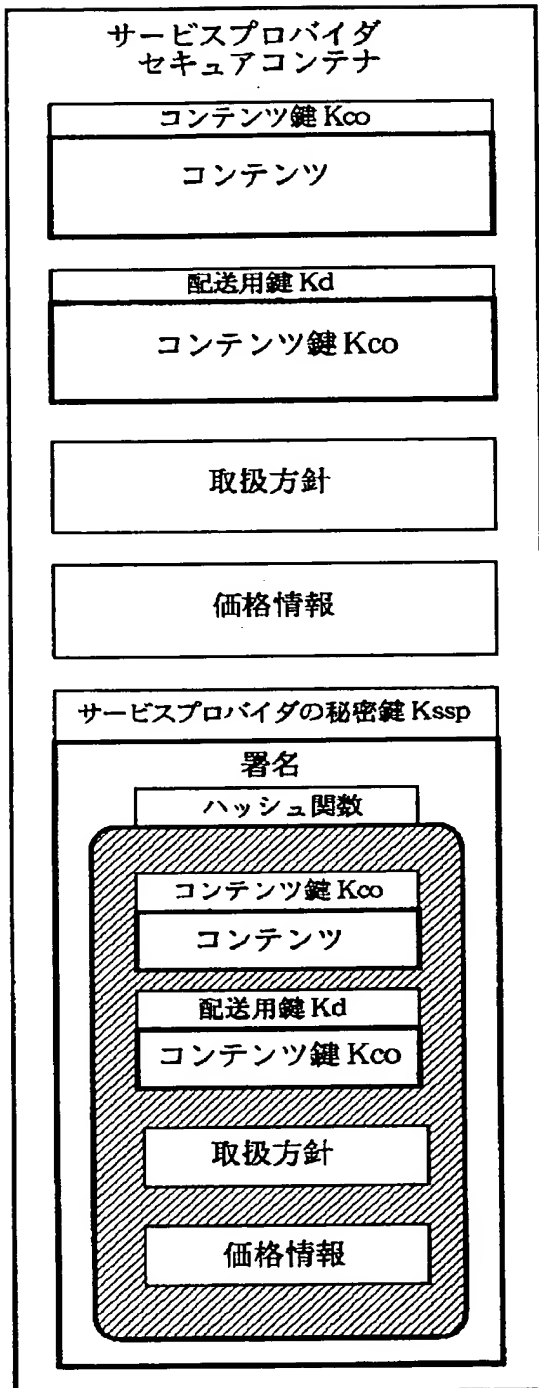
【図 14】



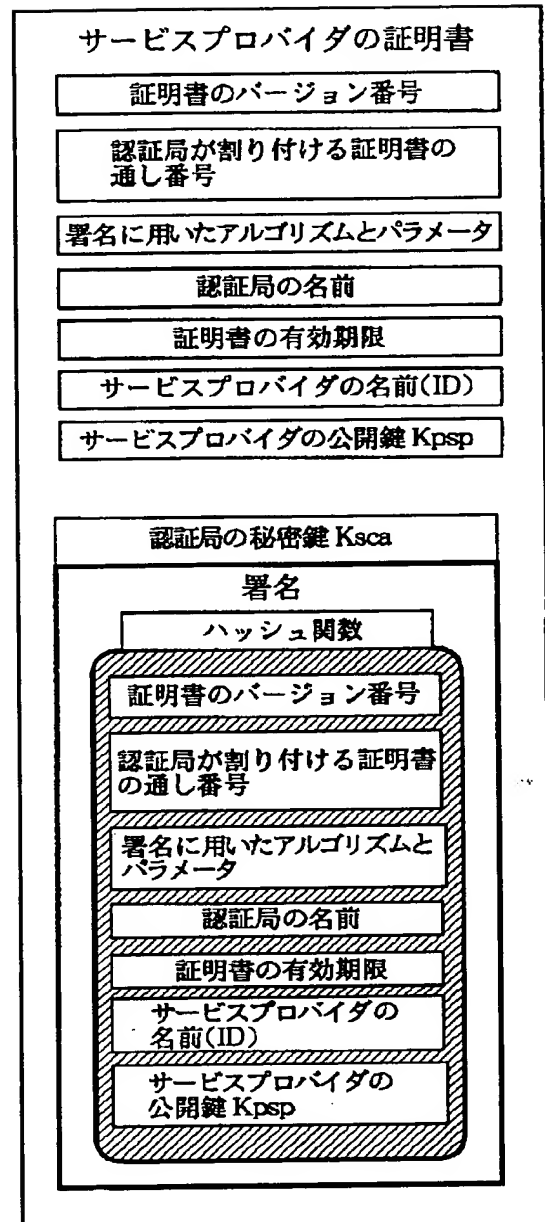
【図 29】

プロバイダ ID	コンテンツ ID	割引率	期間
コンテンツプロバイダ 1	1	0.02	1998.9~1998.12
	2	0.03	
	すべてのコンテンツ	0.01	
コンテンツプロバイダ 2	3	0.05	
サービスプロバイダ 1	1	0.03	
サービスプロバイダ 2	4	0.01	

【図 15】



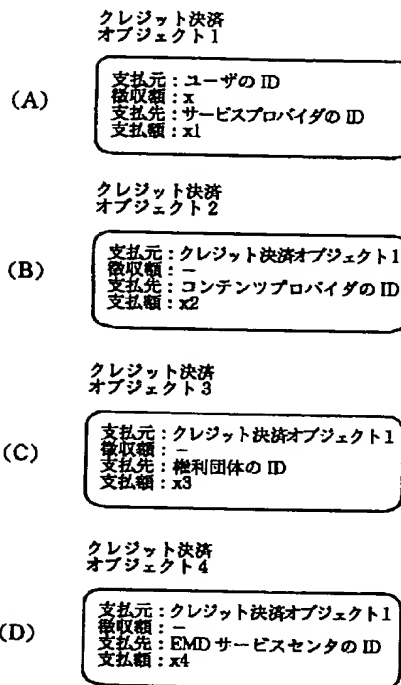
【図 16】



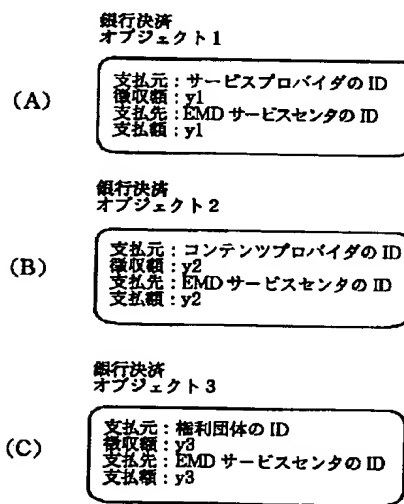
【図 30】

月額固定額	変動額		
1000 円	期間	1998. 8. ~1998. 9	-10%
	利用料	3000 円以上	-5%

【図 5 8】

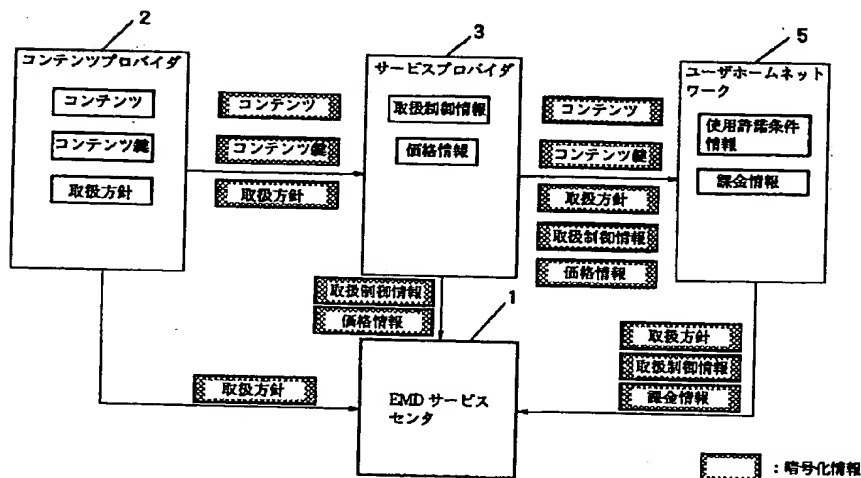


【図 5 9】



(C)

銀行決済 オブジェクト 3
支払元: 権利団体の ID
徴収額: y3
支払先: EMD サービスセンタの ID
支払額: y3



【図19】

(A) 取扱方針
利益分配

利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	70 円	-	40 円

(B) 取扱方針
利益分配
価格情報


利用内容	再生	シングルコピー	マルチコピー
可/否	1	0	1
利益分配	60 円	-	30 円
分配価格	150 円	-	80 円

(C) 課金情報


利用内容	再生	シングルコピー	マルチコピー
利用回数	1	0	0

【図20】

(A)	取扱方針 および 価格情報	再生		
		制限なし	回数制限	期日制限
		-	5	1998/12/31
		価格	-	80 円



(B)	使用許諾条件 情報	再生		
		制限なし	回数制限	期日制限
		-	5	-
		3 回再生後		

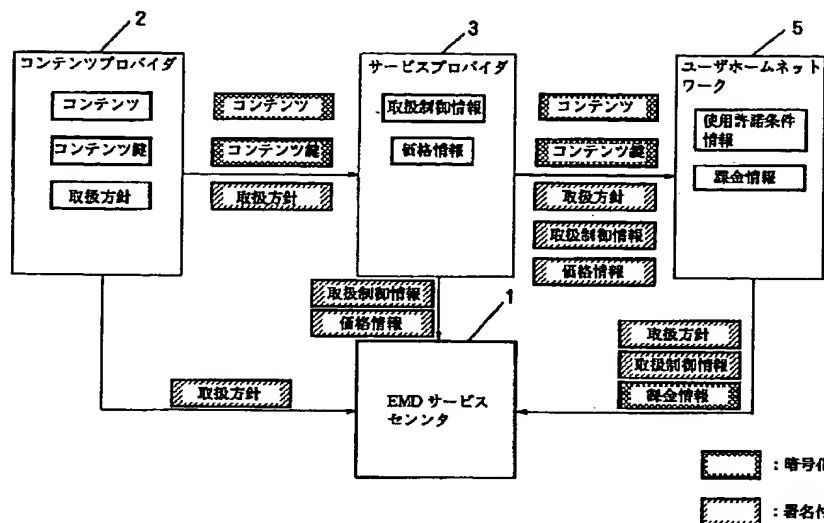


(C)	使用許諾条件 情報	再生		
		制限なし	回数制限	期日制限
		-	2	-

【図42】

SAM の ID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

【図 21】



【図 60】

クレジット決済
オブジェクト 1

(A)

支払元: ユーザの ID
 徴収額: x
 支払先: サービスプロバイダの ID
 支払額: $x1$

銀行決済
オブジェクト 2

(B)

支払元: サービスプロバイダの ID
 徴収額: $x2+x3$
 支払先: コンテンツプロバイダの ID
 支払額: $x2+x3$

銀行決済
オブジェクト 3

(C)

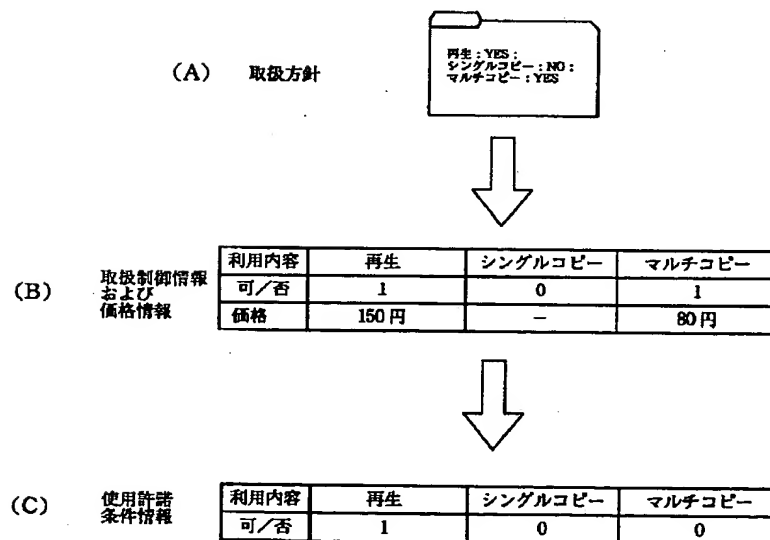
支払元: コンテンツプロバイダの ID
 徴収額: $x3$
 支払先: 権利団体の ID
 支払額: $x3$

クレジット決済
オブジェクト 4

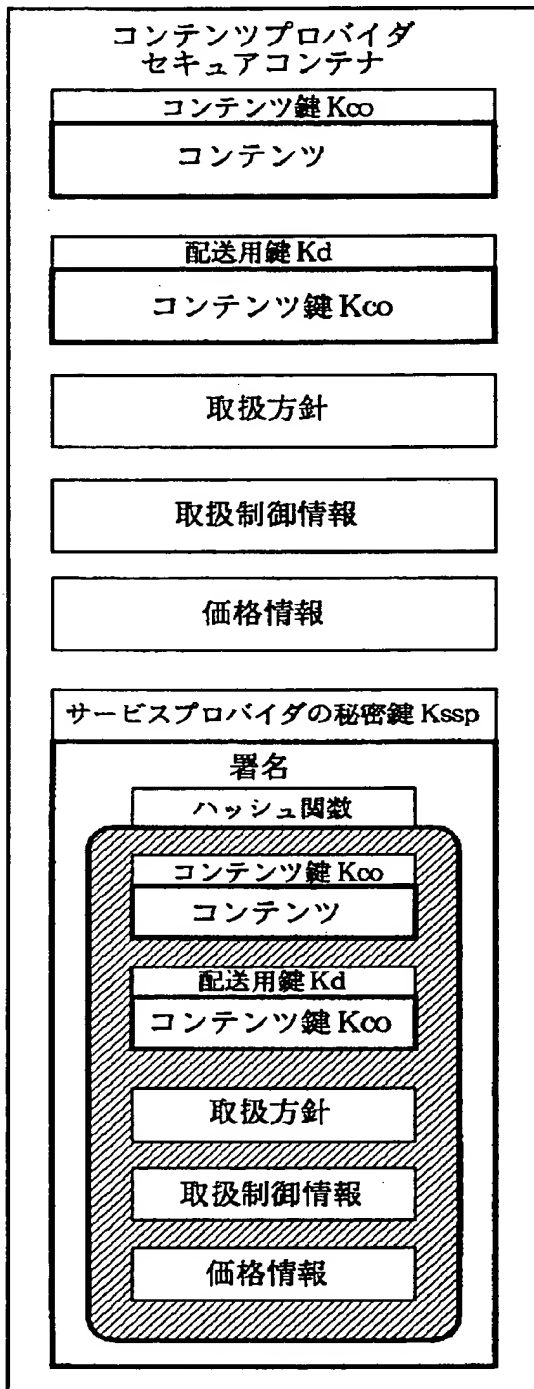
(D)

支払元: クレジット決済オブジェクト 1
 徴収額: $-$
 支払先: EMD サービスセンタの ID
 支払額: $x4$

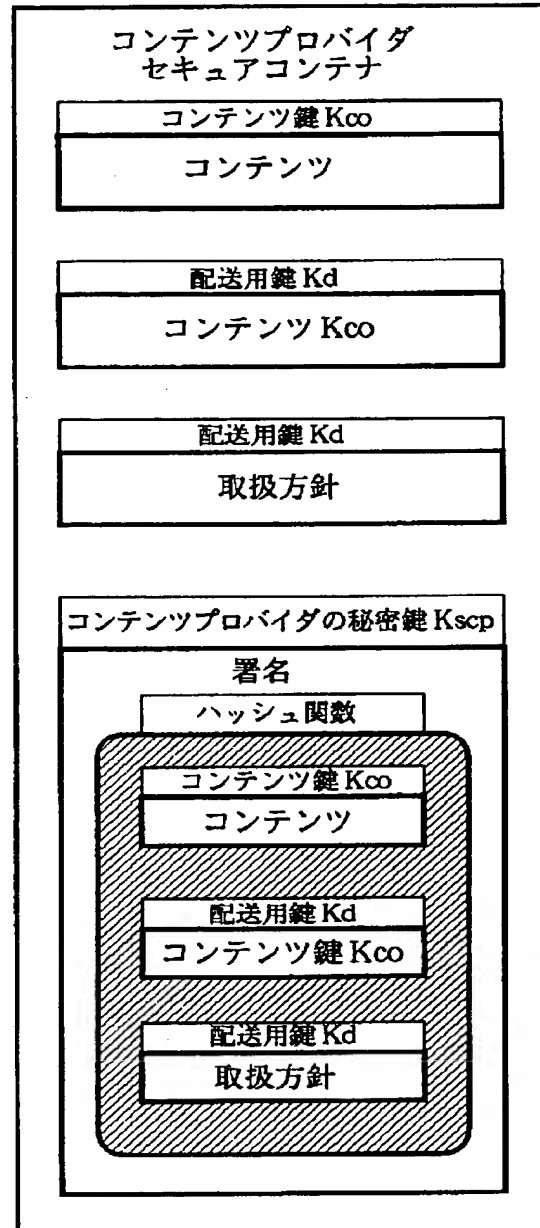
【図 23】



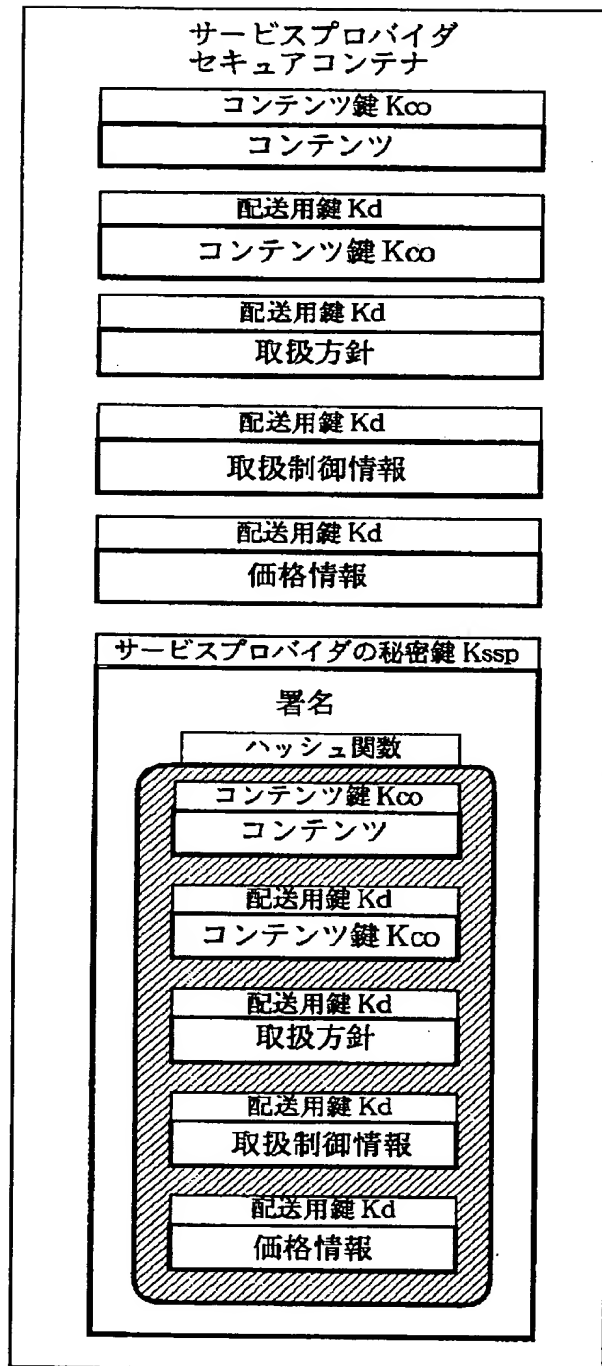
【図 22】



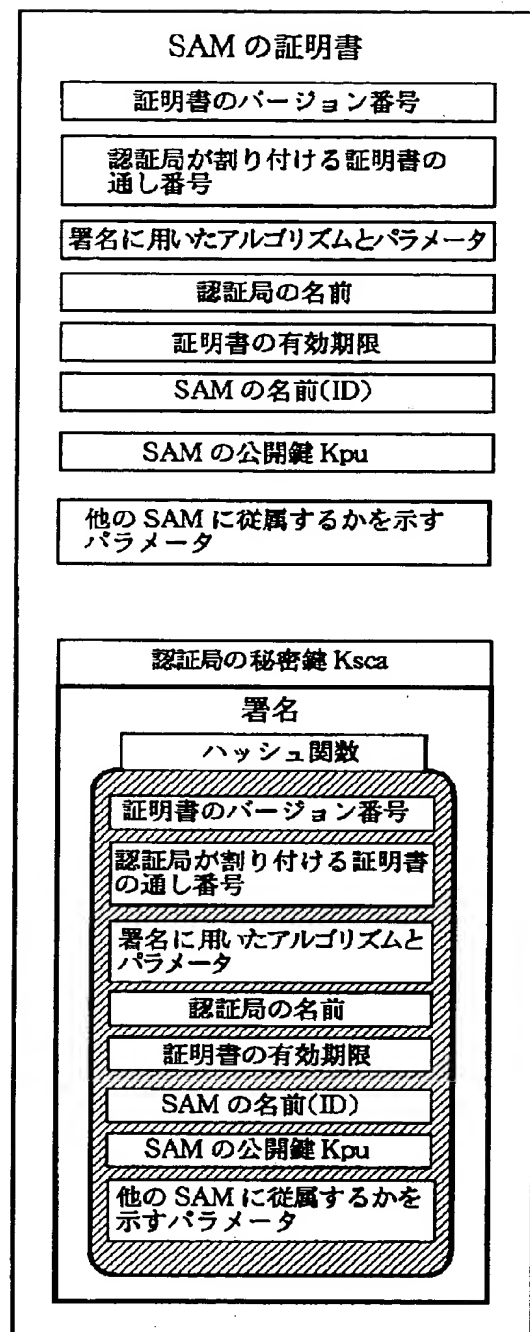
【図 25】



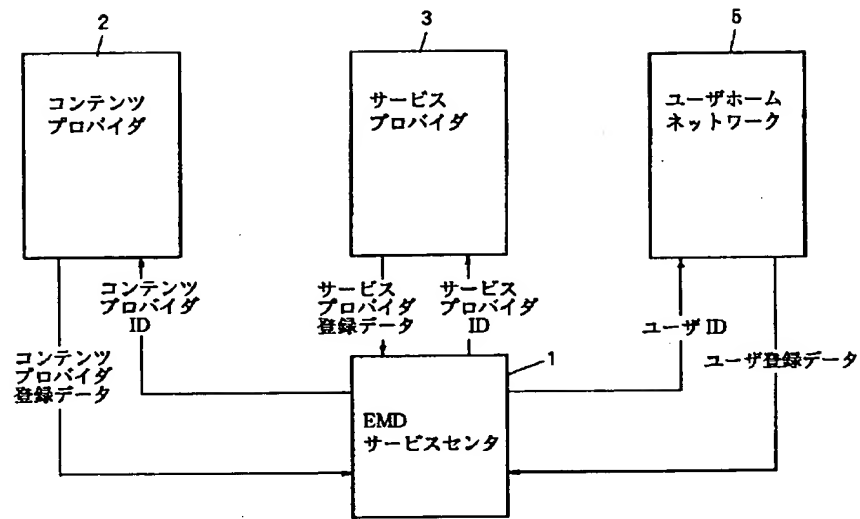
【図 26】



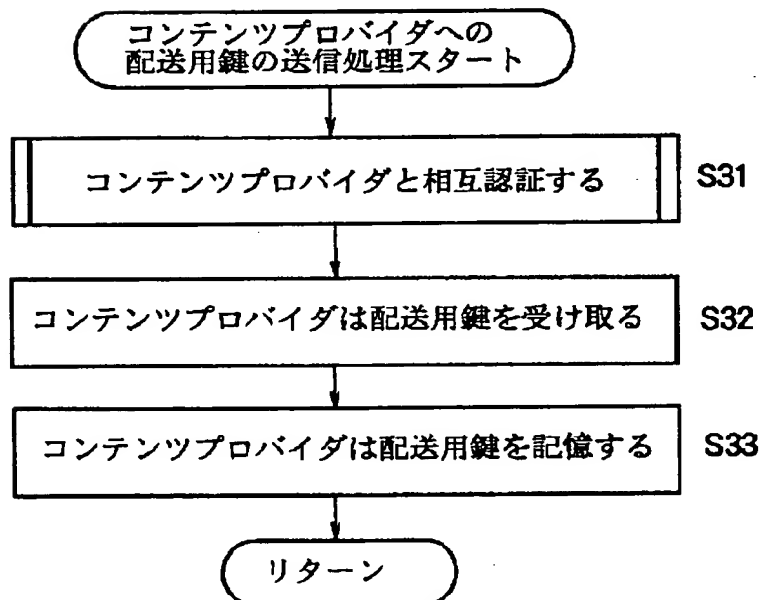
【図 41】



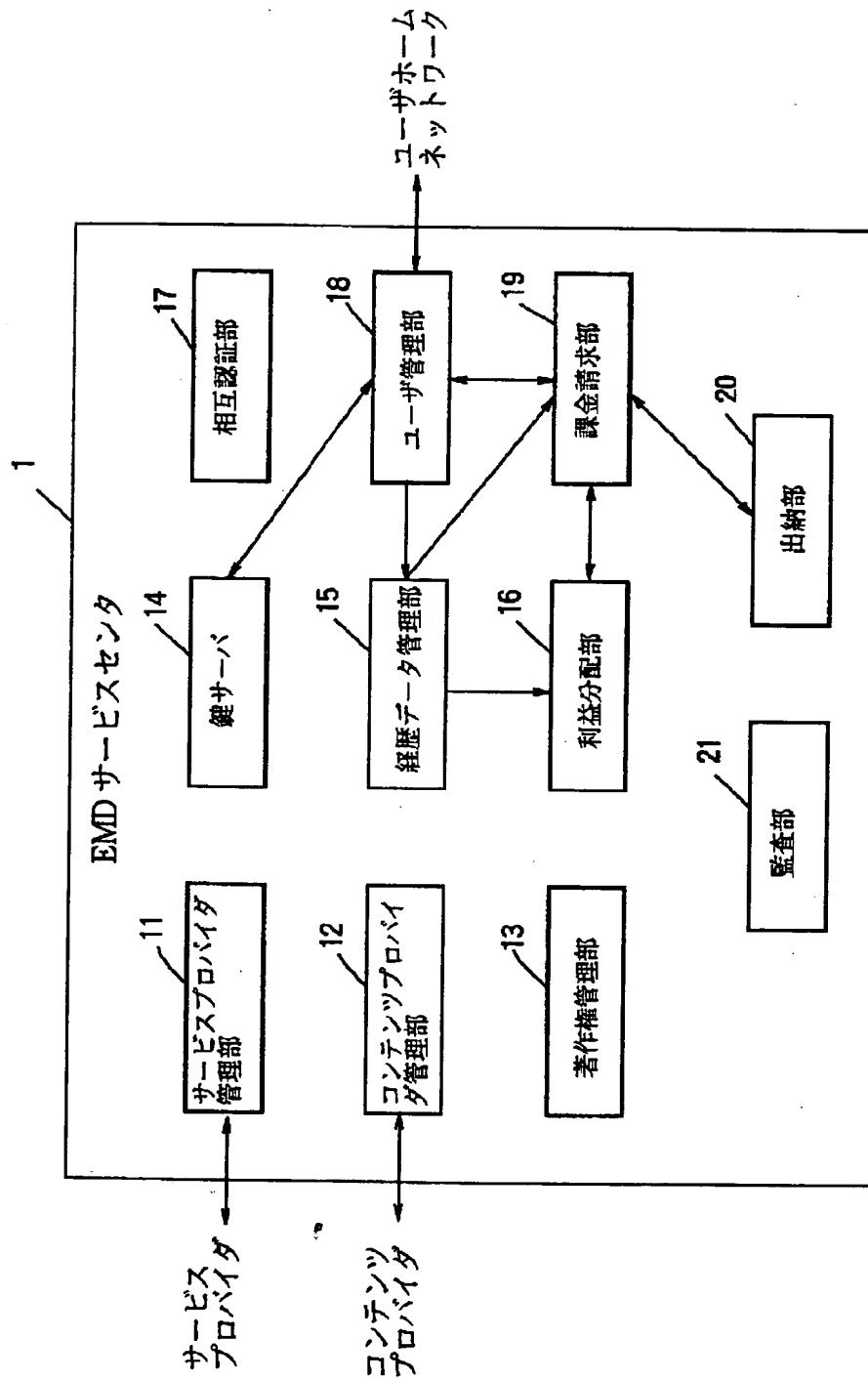
【図27】



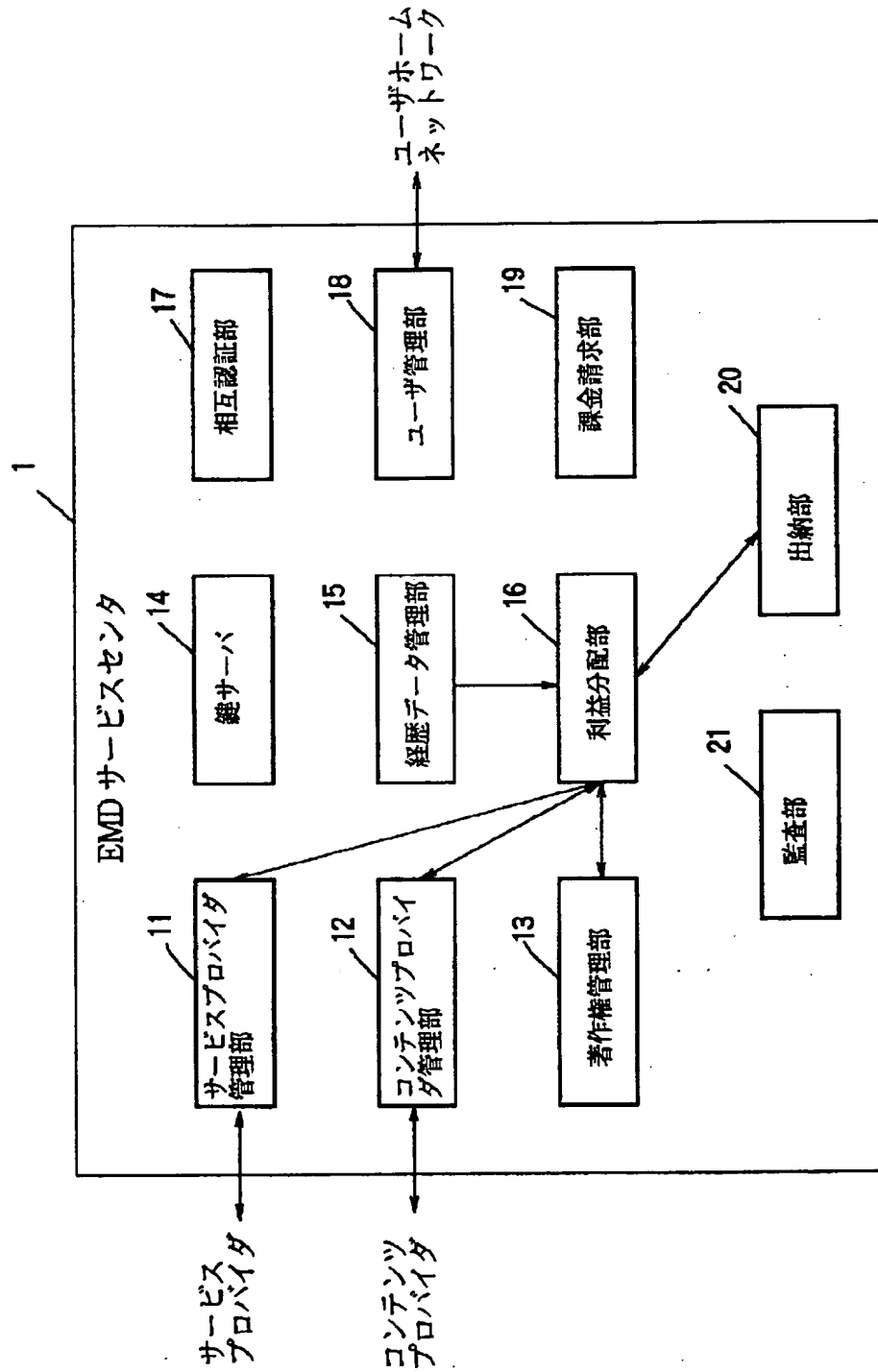
【図36】



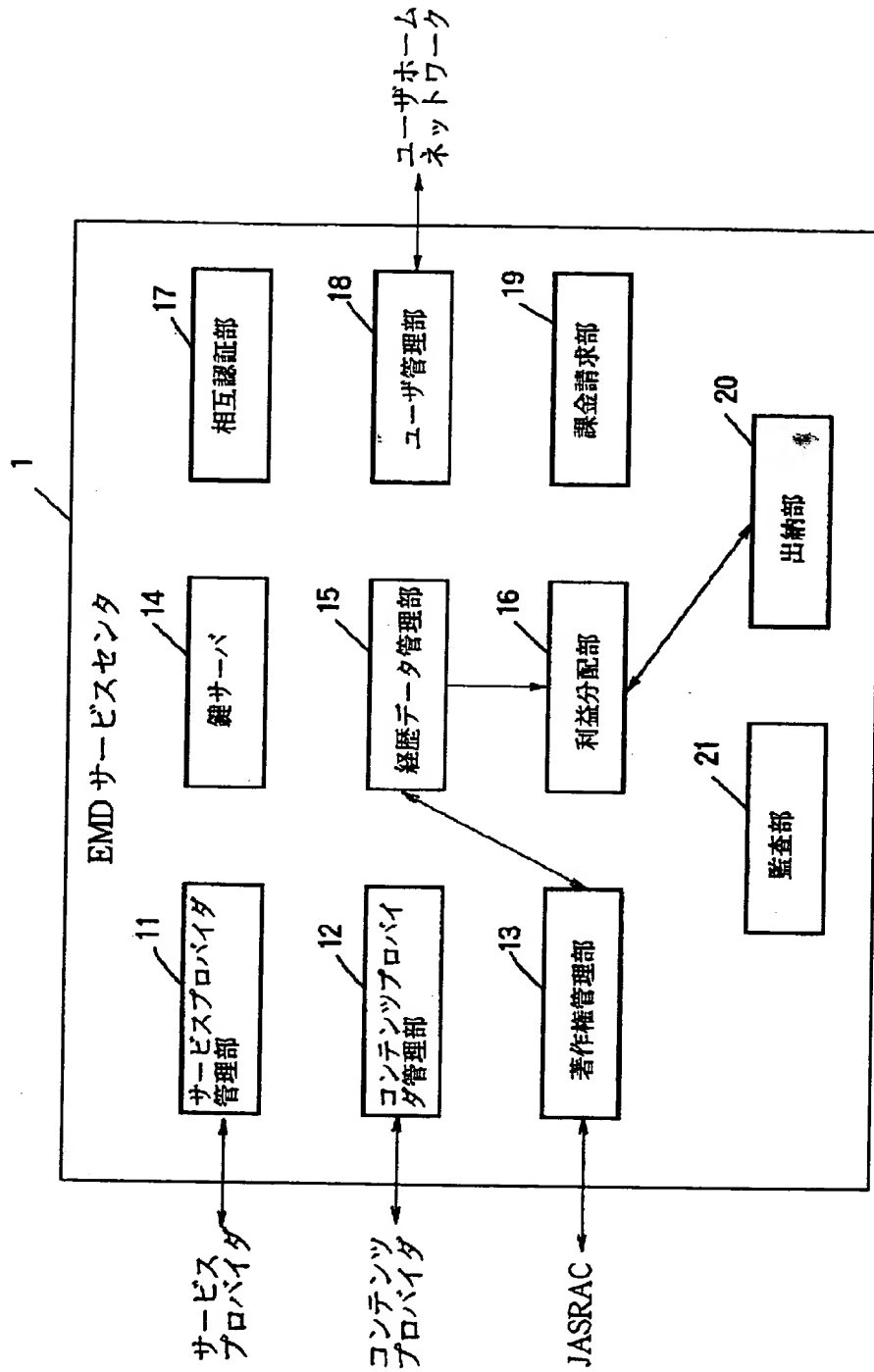
【図 31】



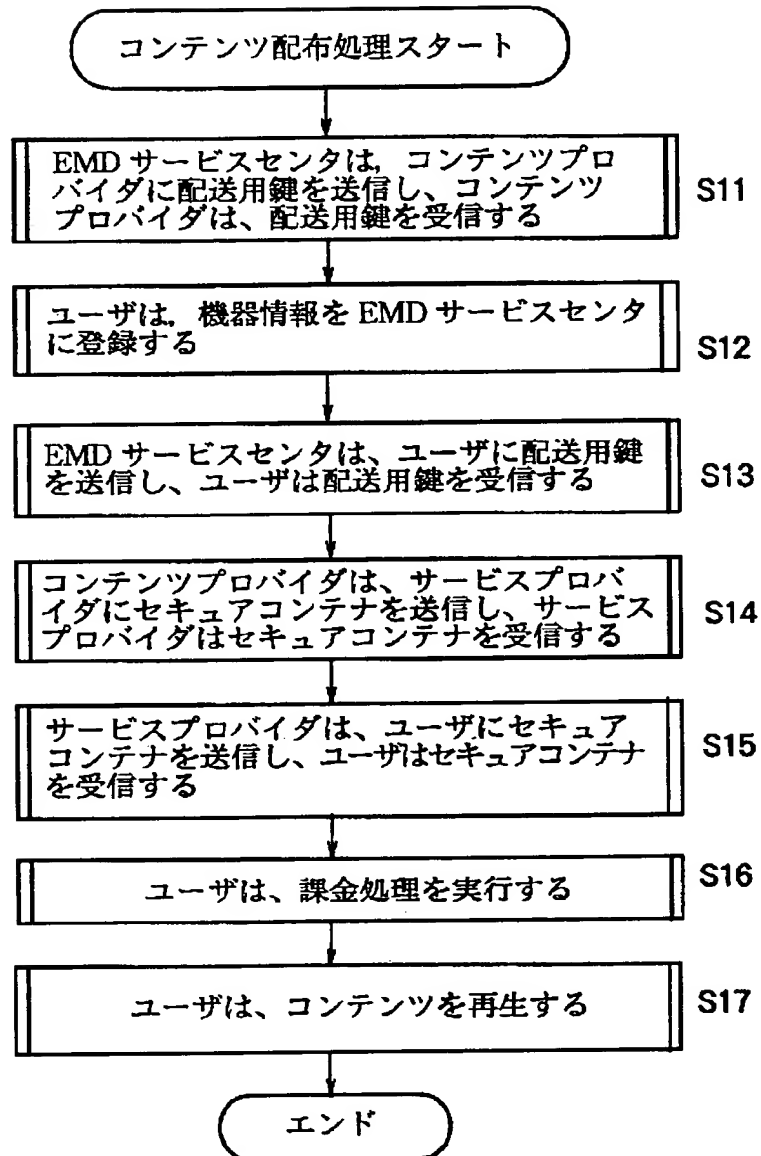
【図 32】



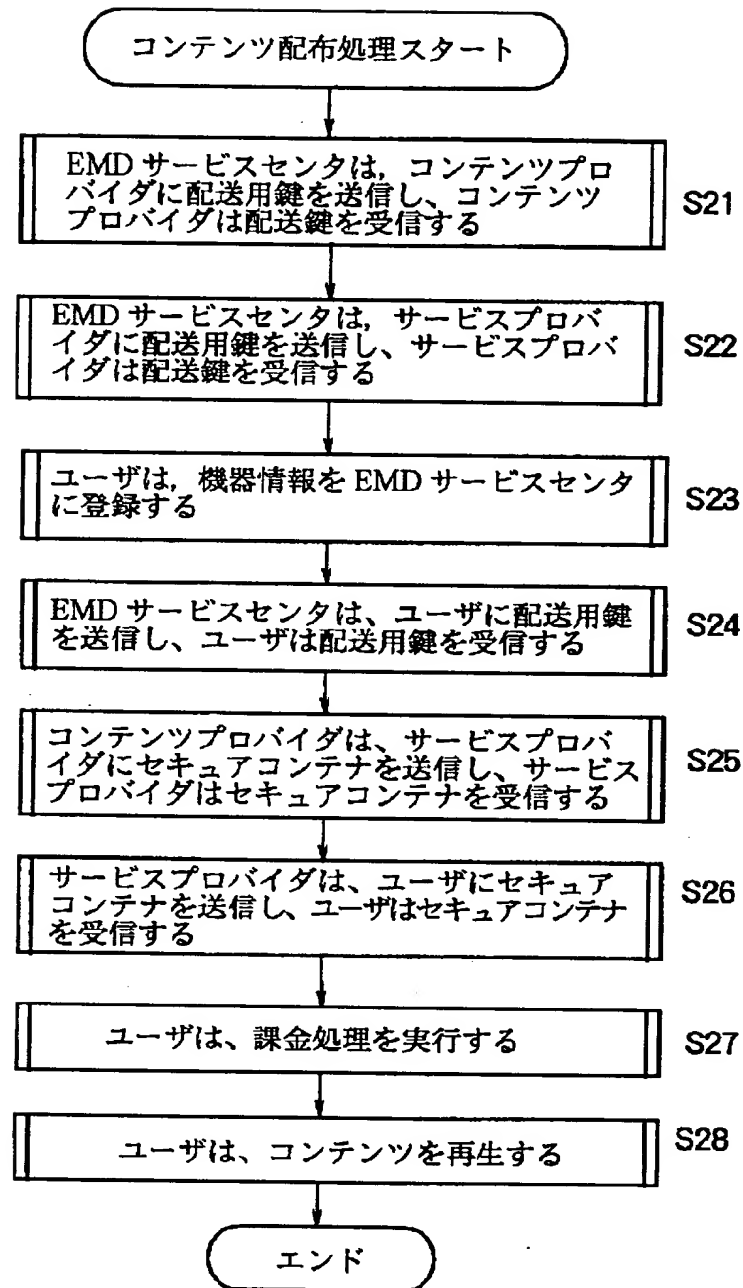
【図 33】



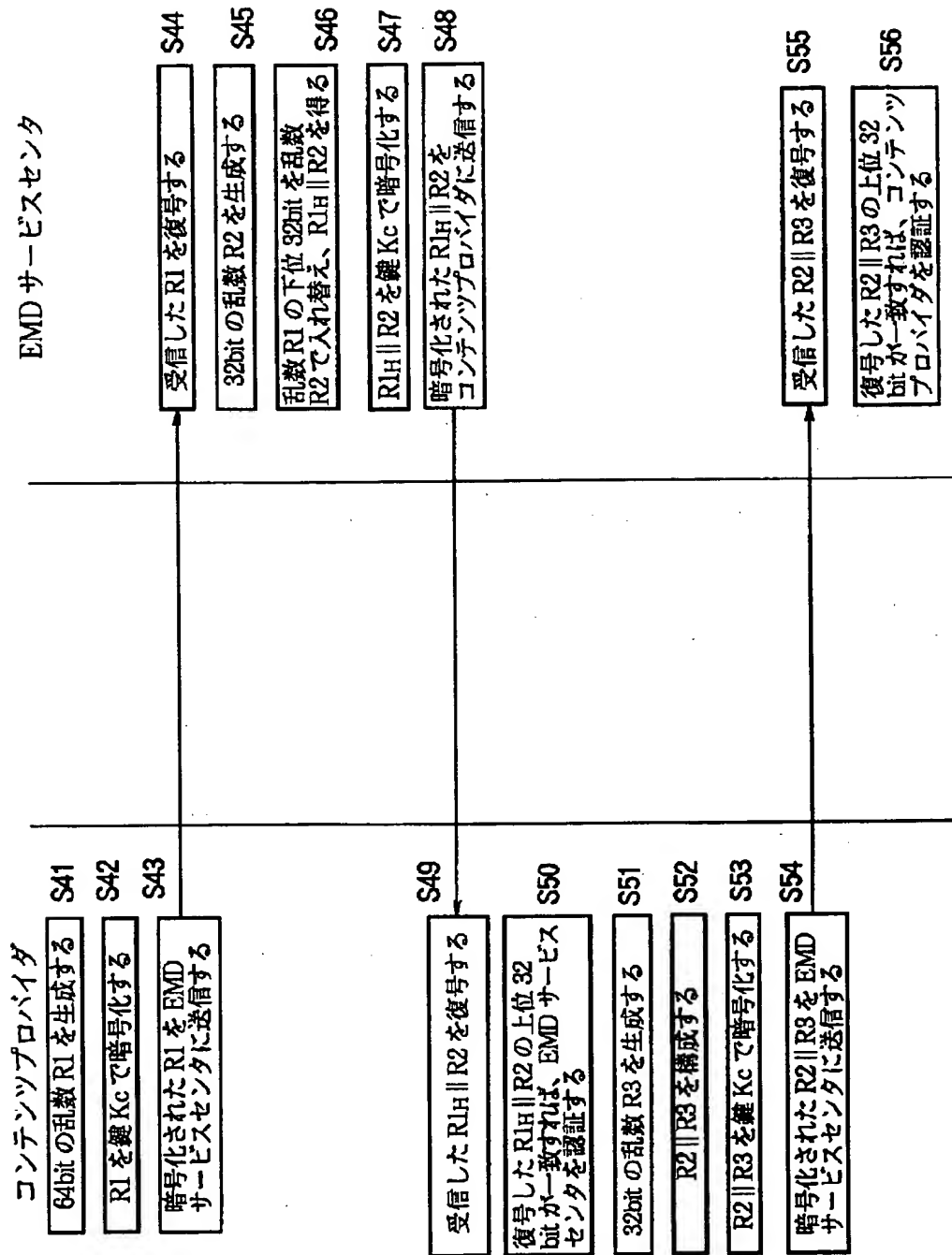
【図 34】



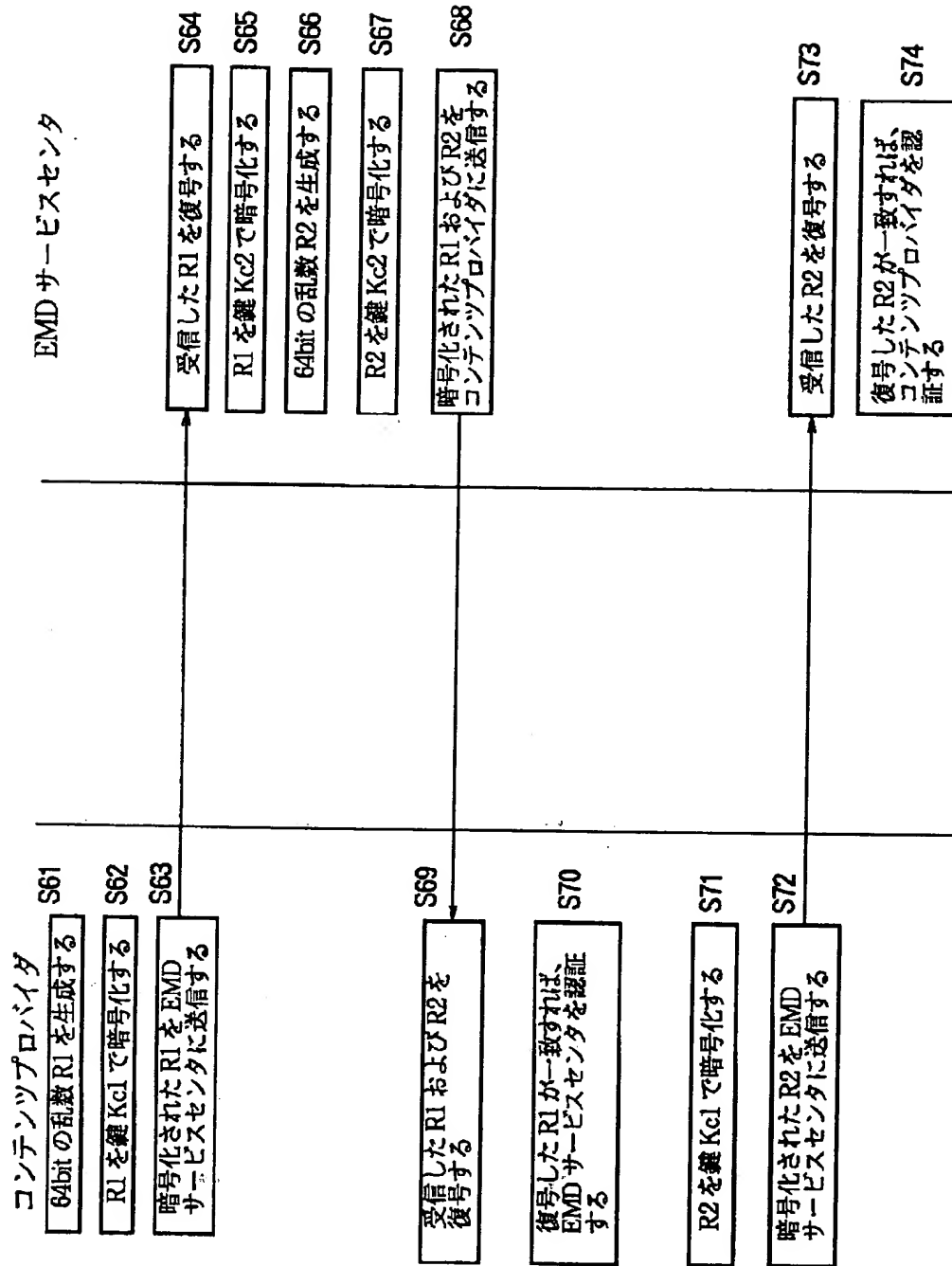
【図35】



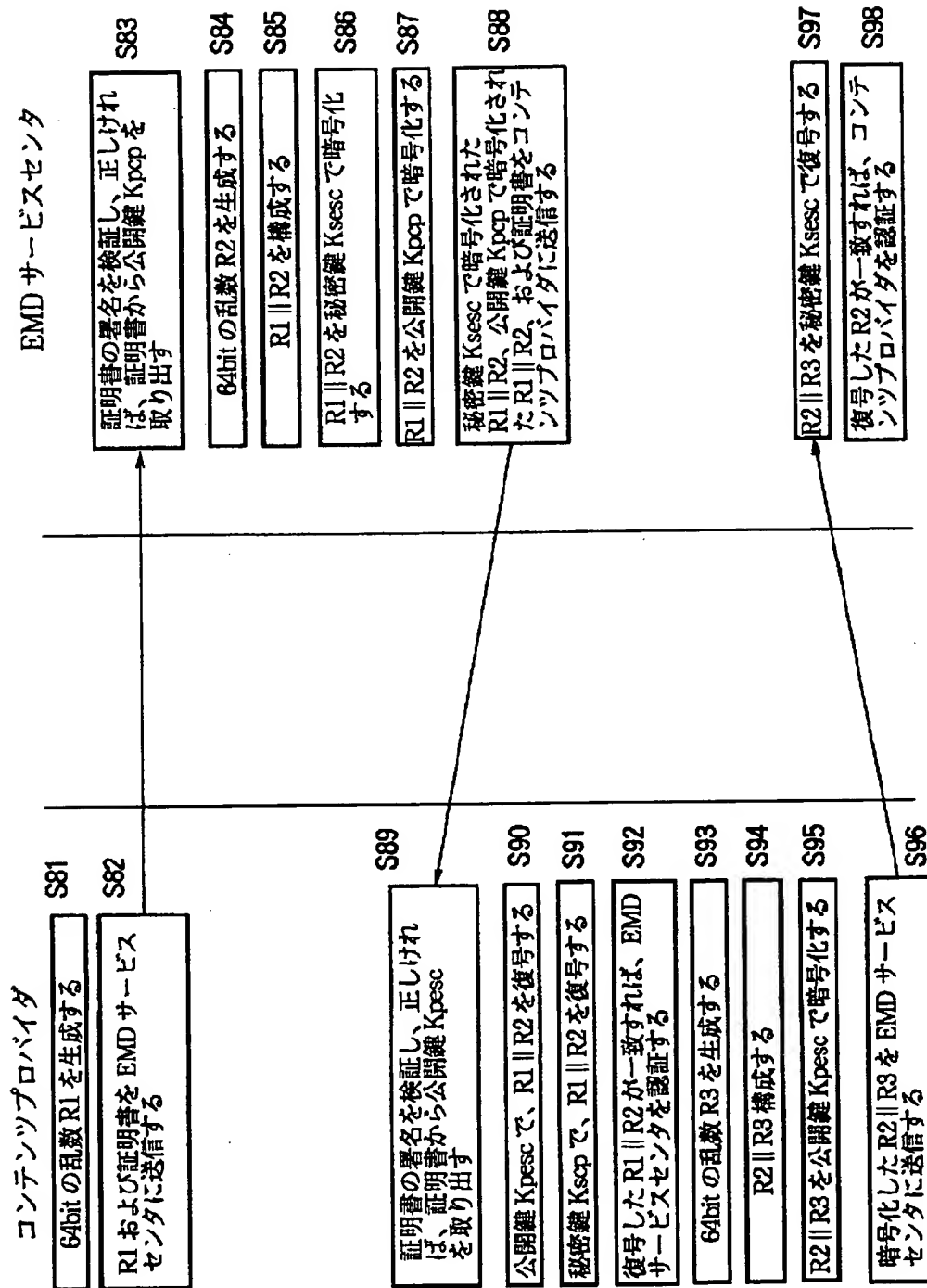
【図 37】



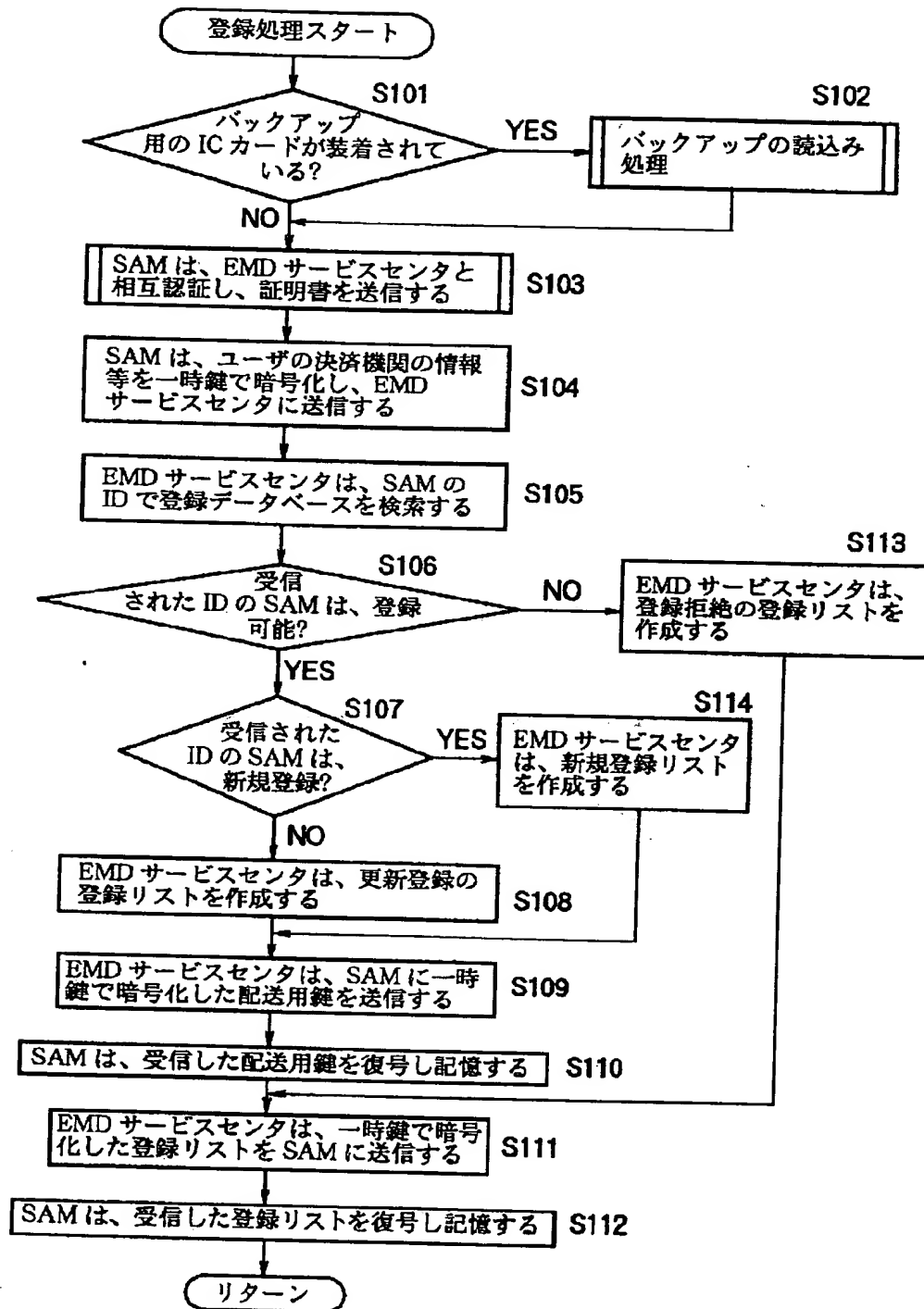
【図38】



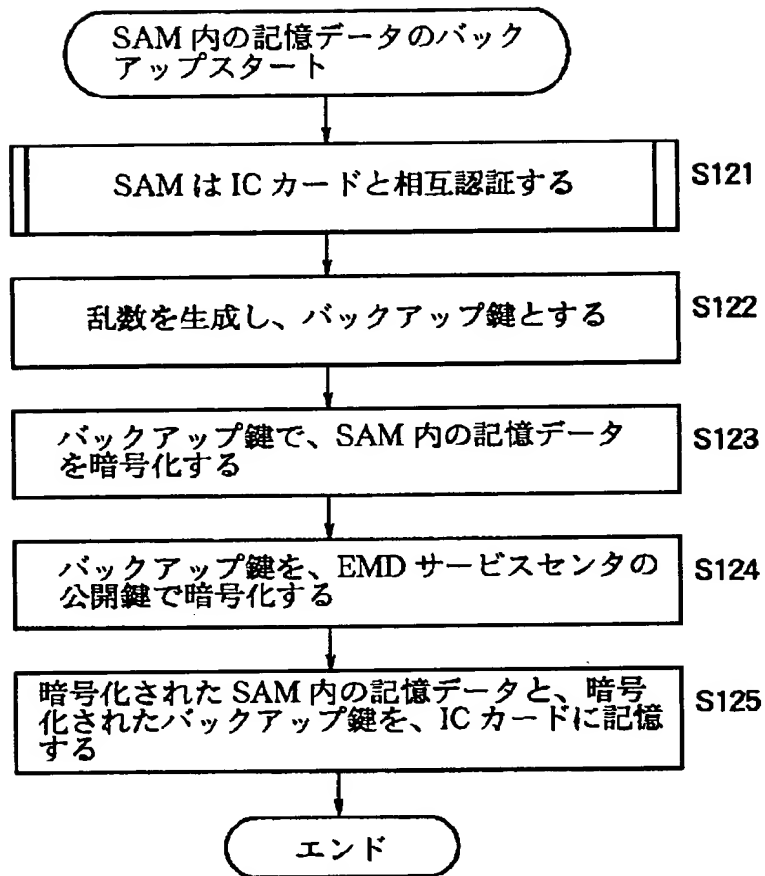
【図39】



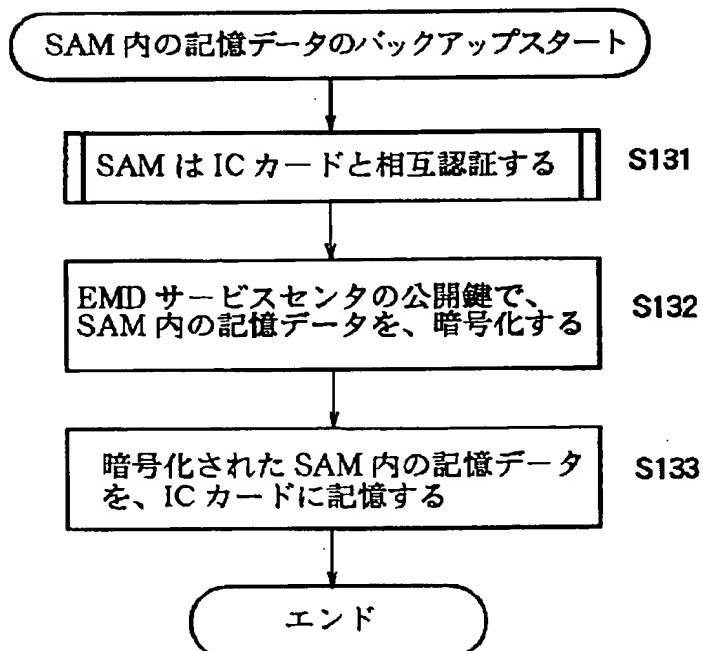
【図 40】



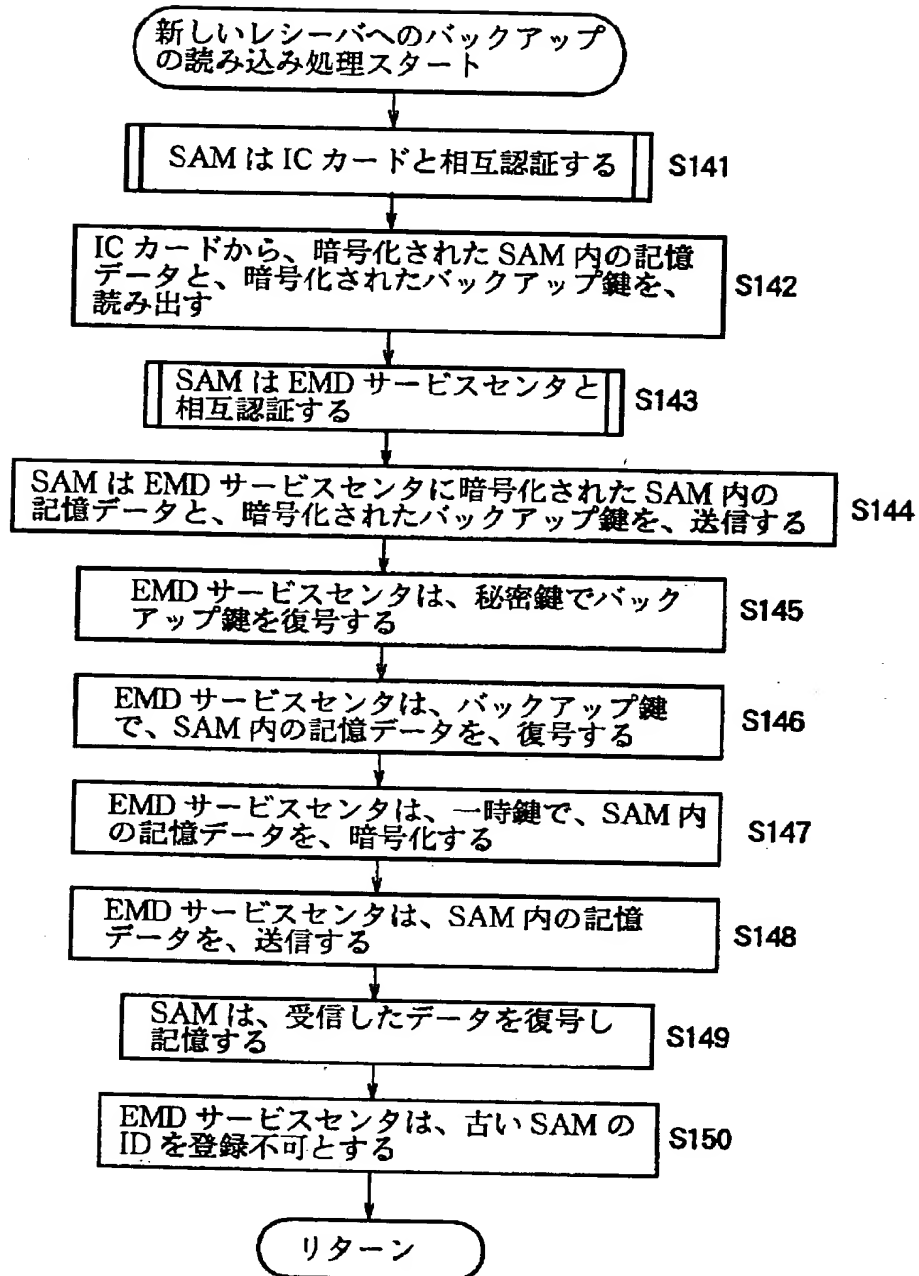
【図 4 3】



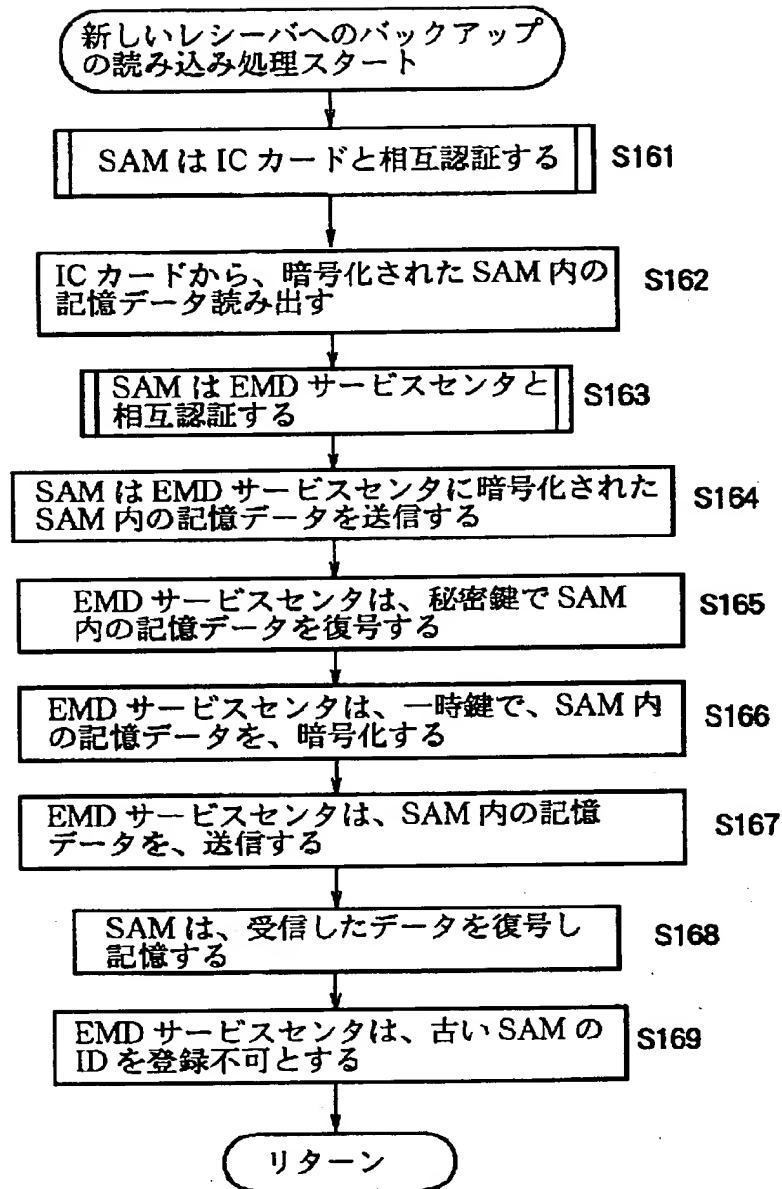
【図 4 4】



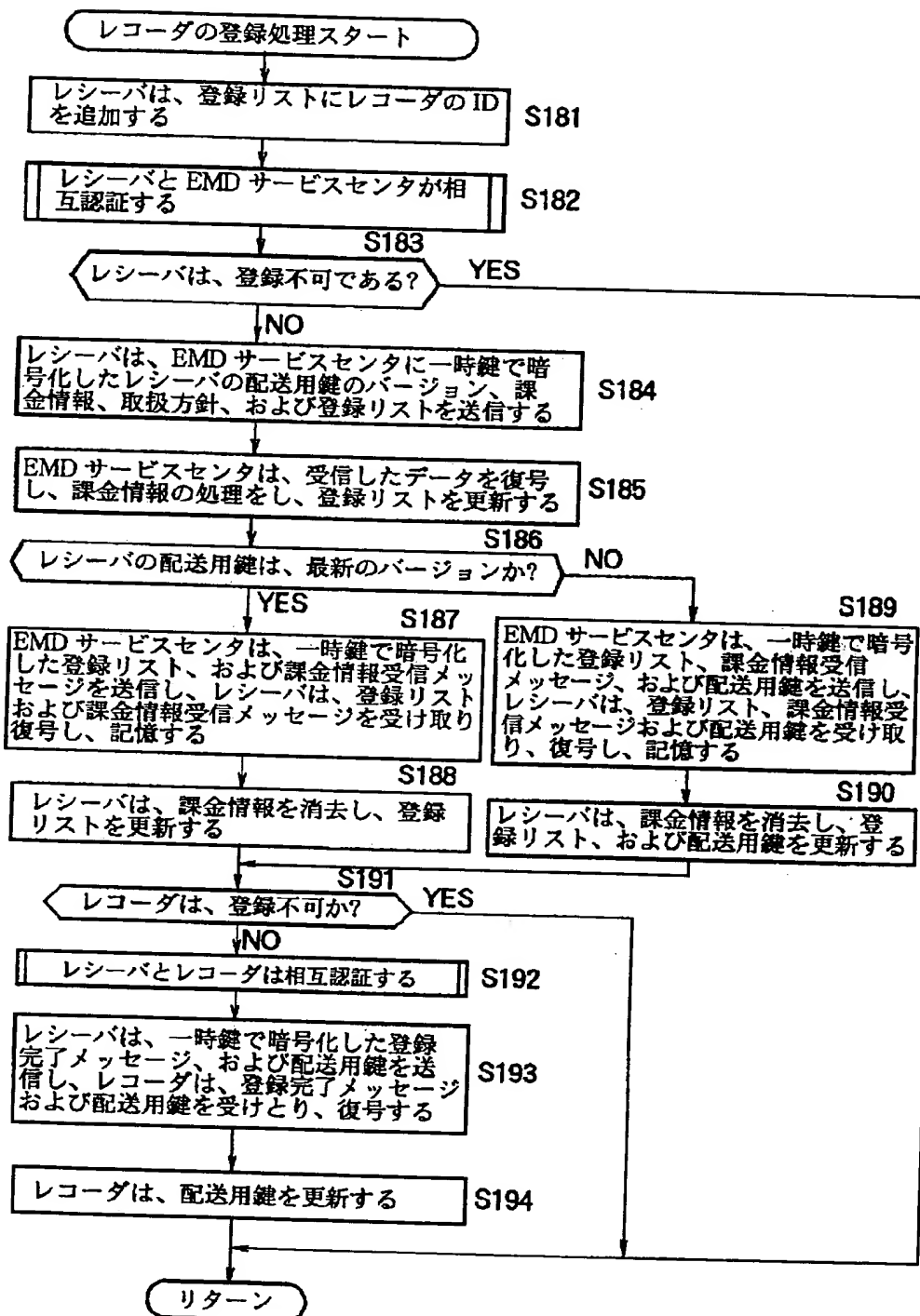
【図 45】



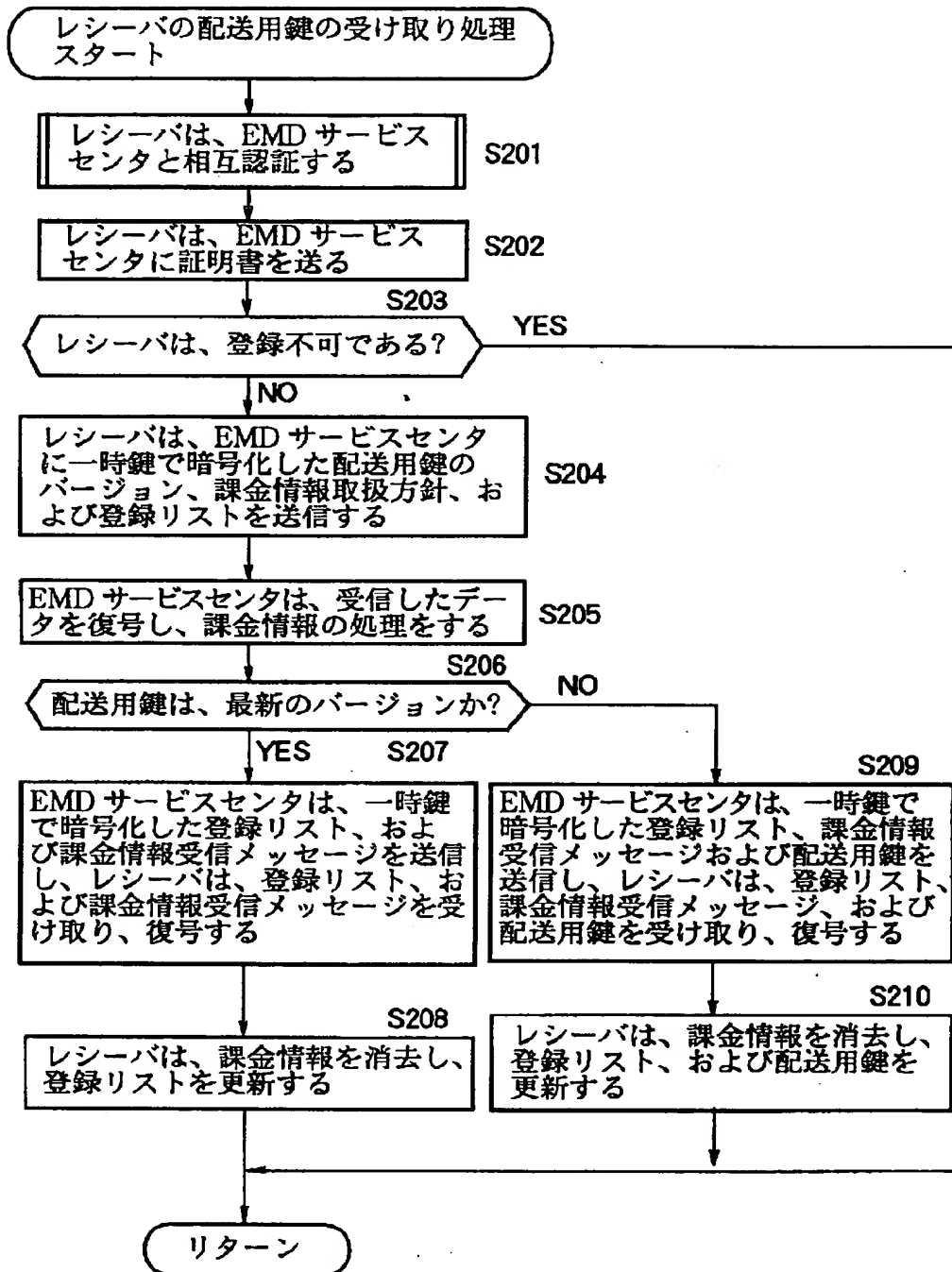
【図46】



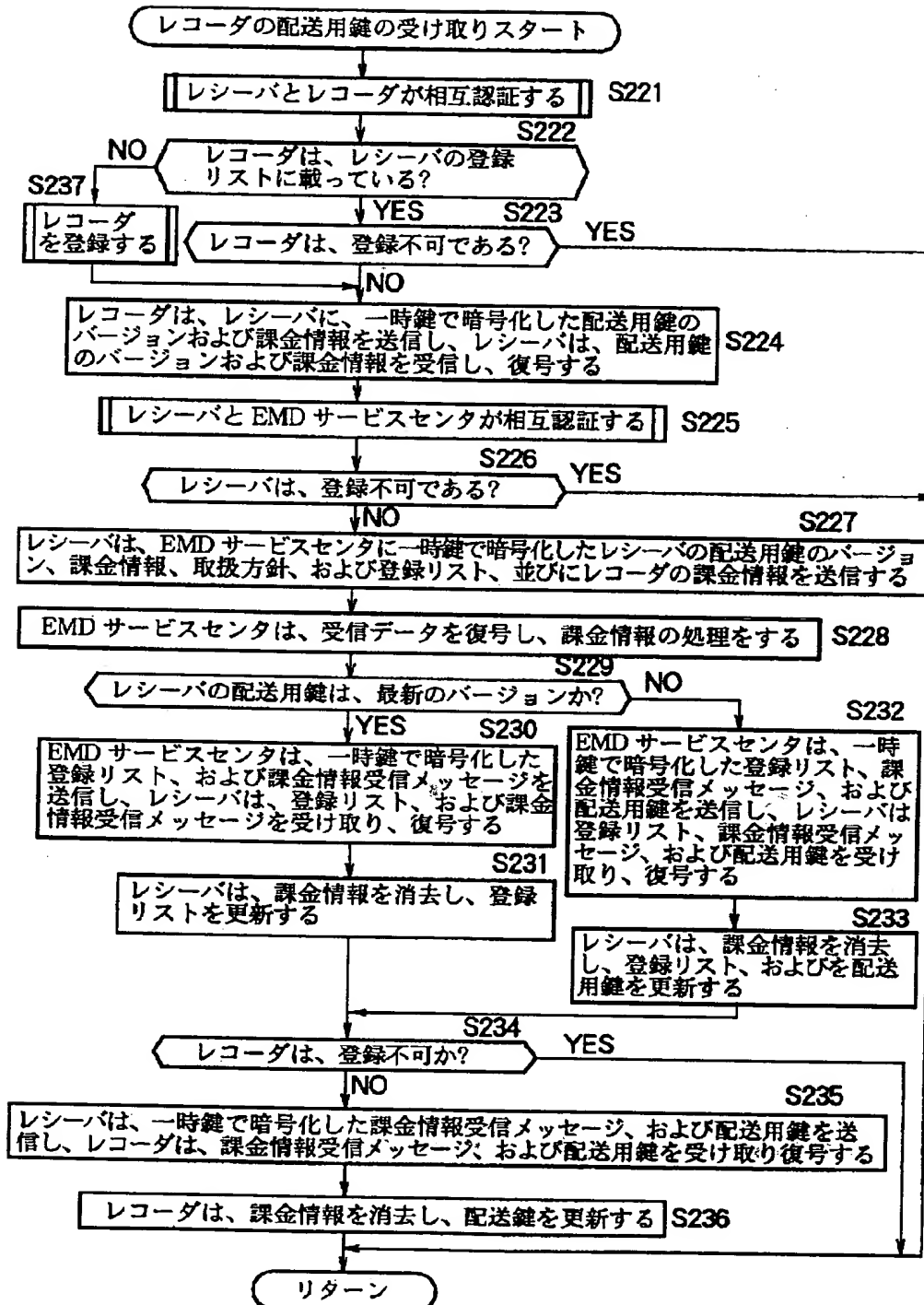
【図 47】



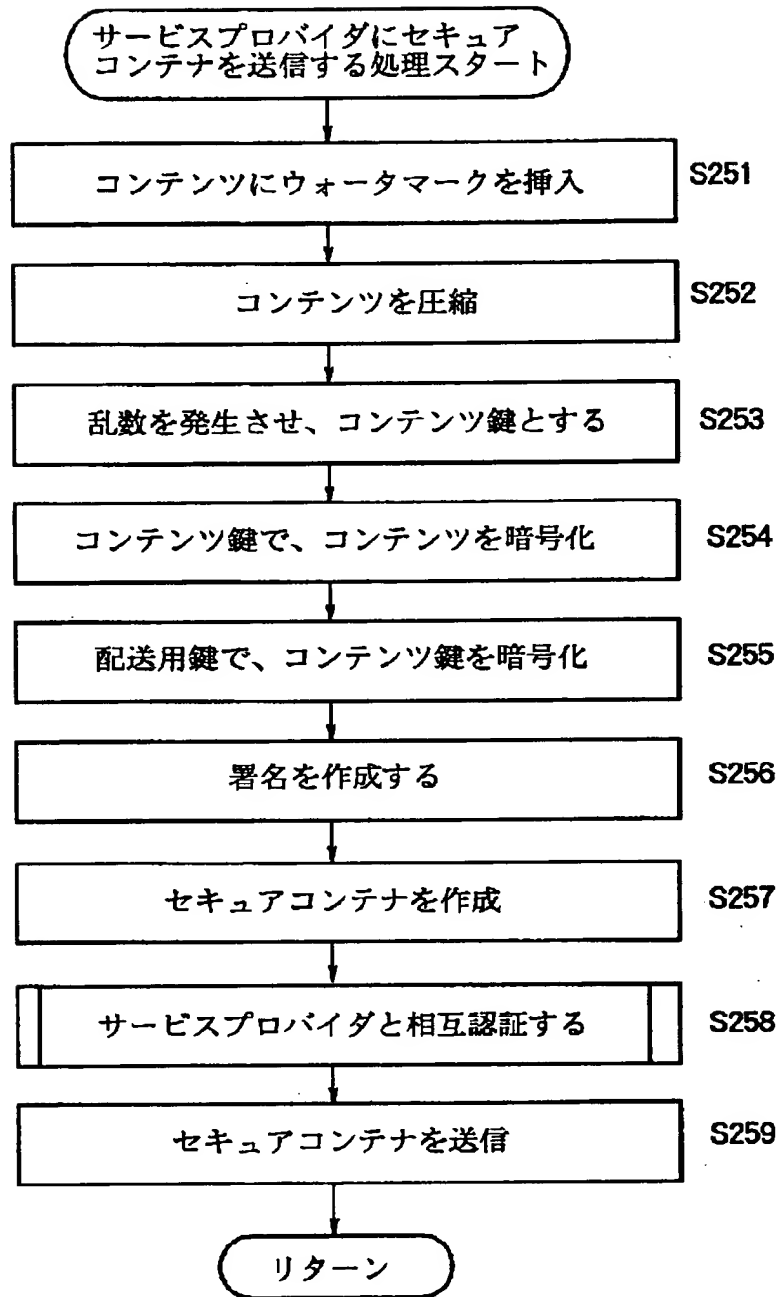
【図 48】



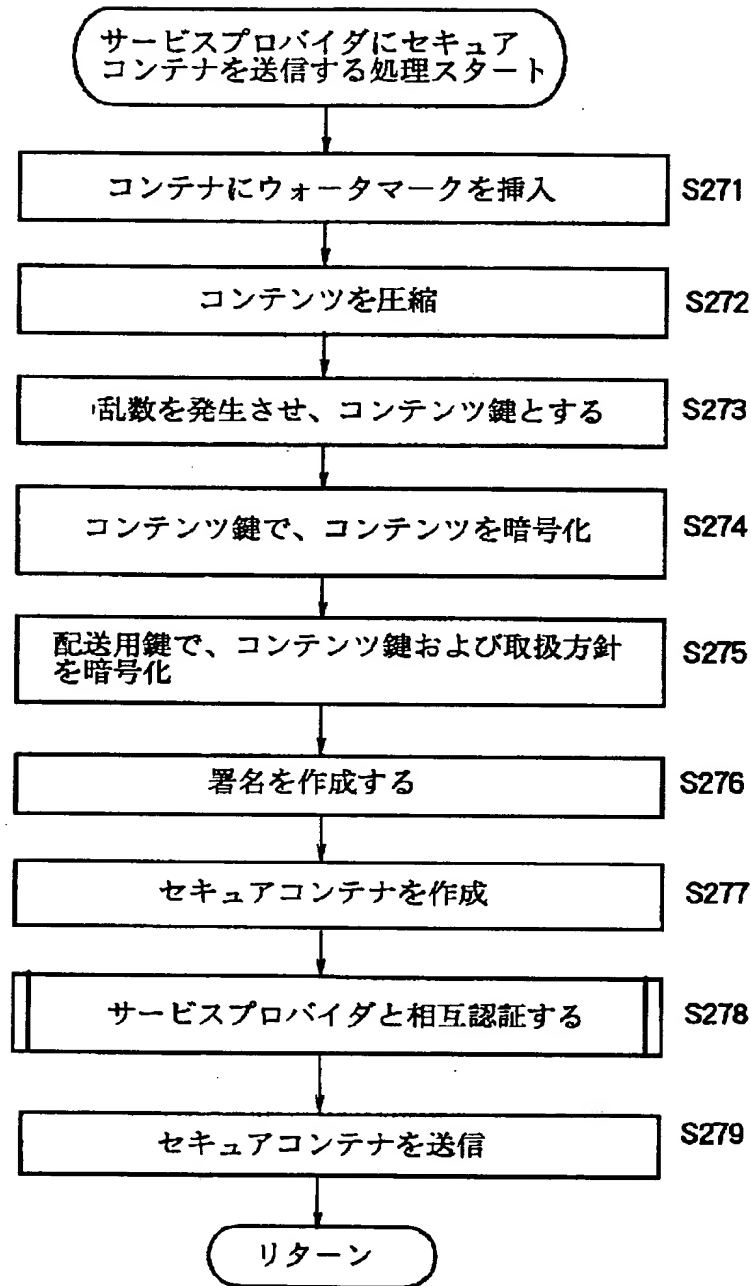
【図49】



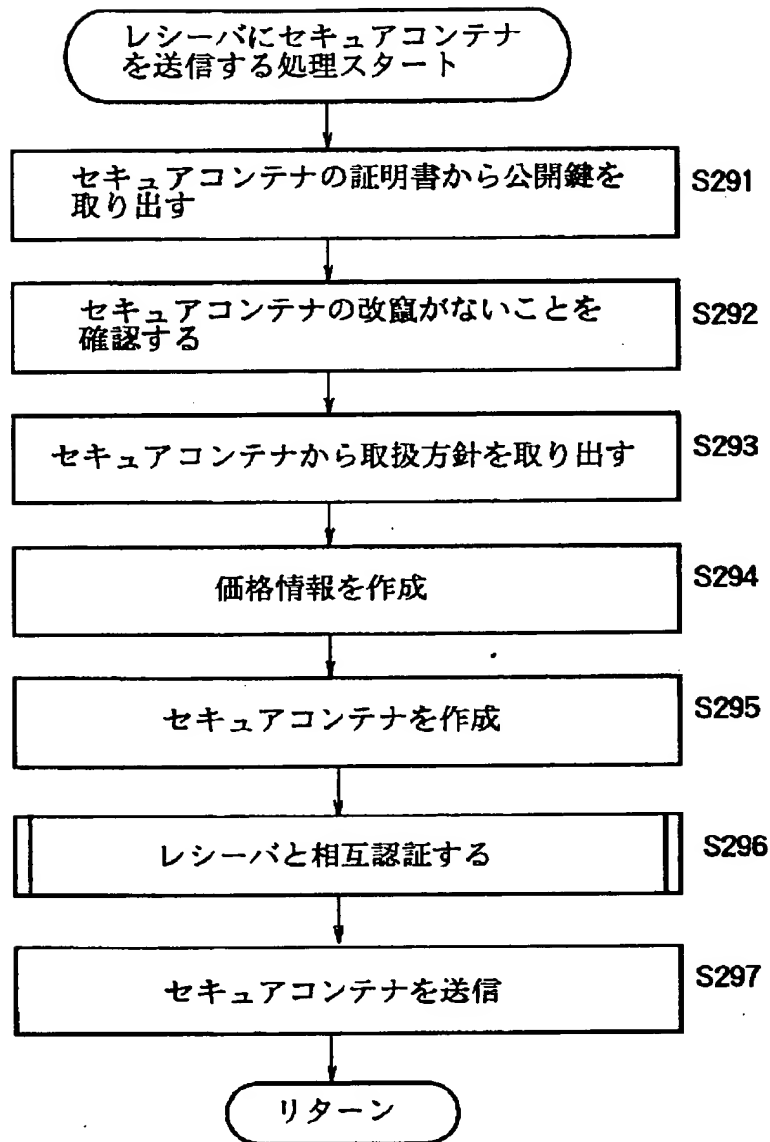
【図 50】



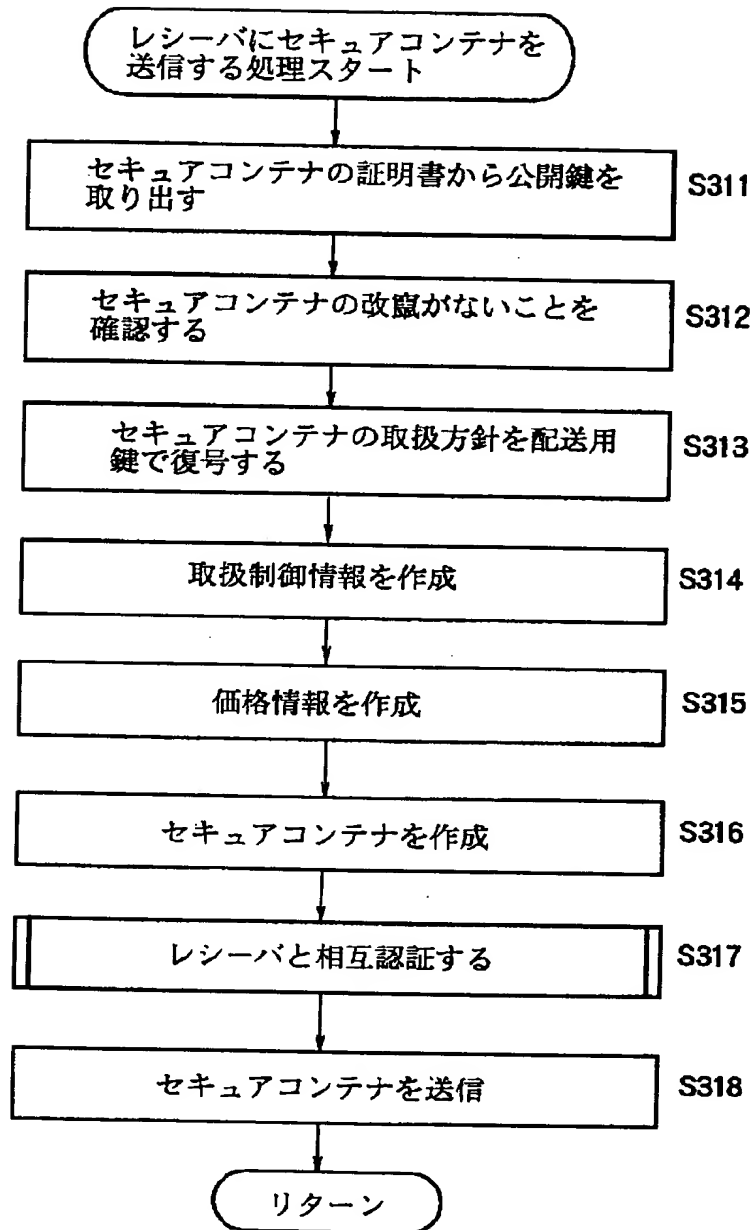
【図 51】



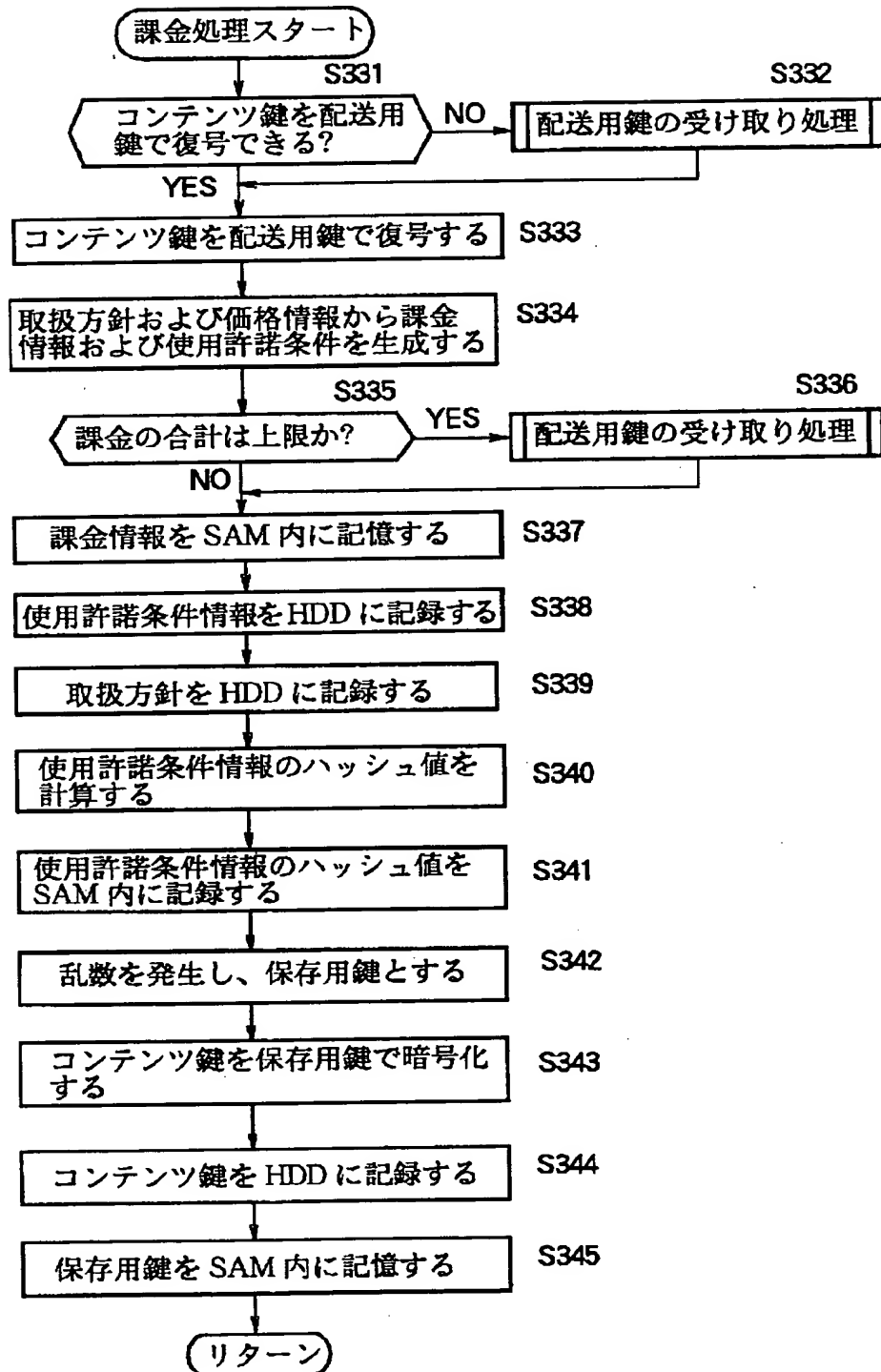
【図 52】



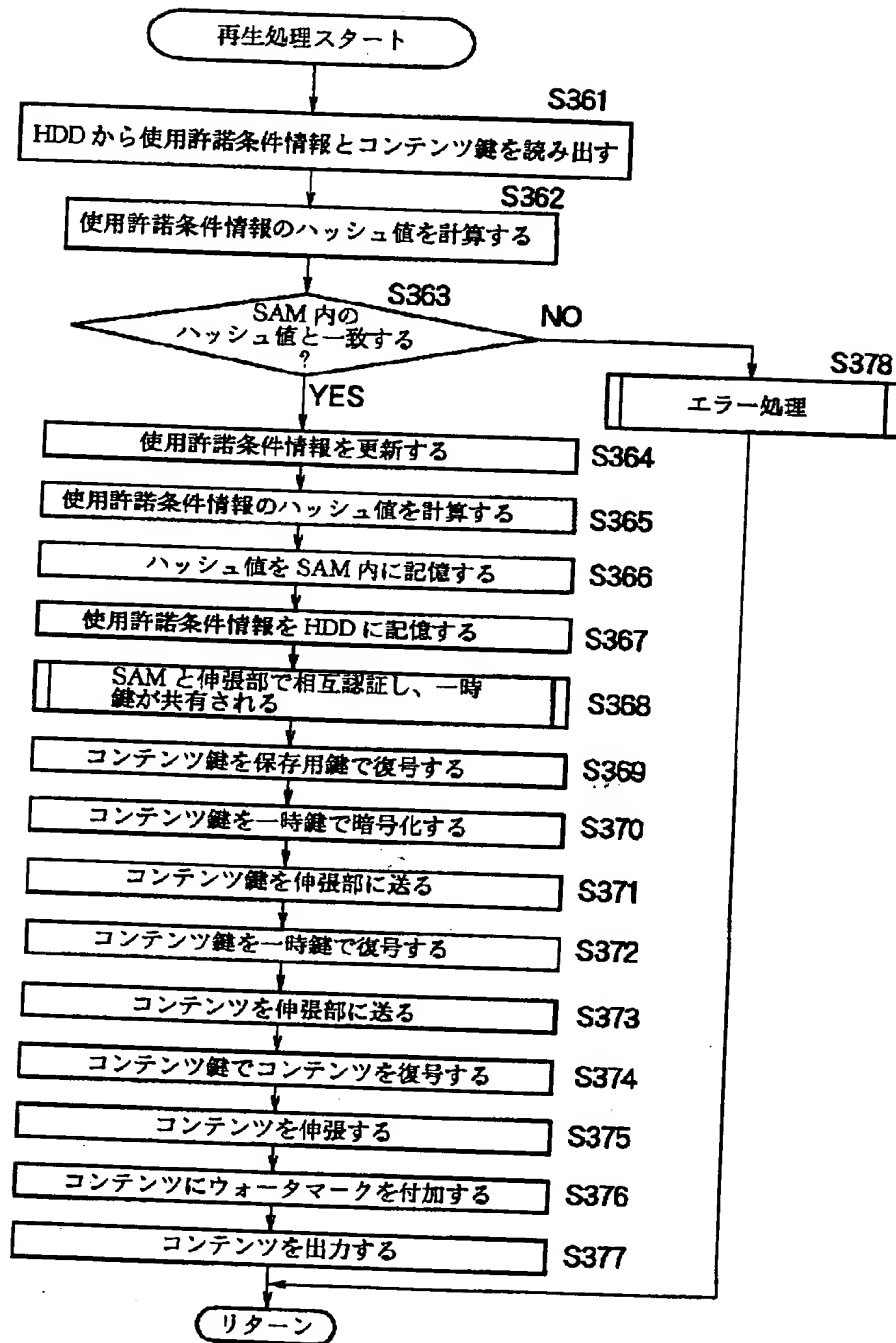
【図 53】



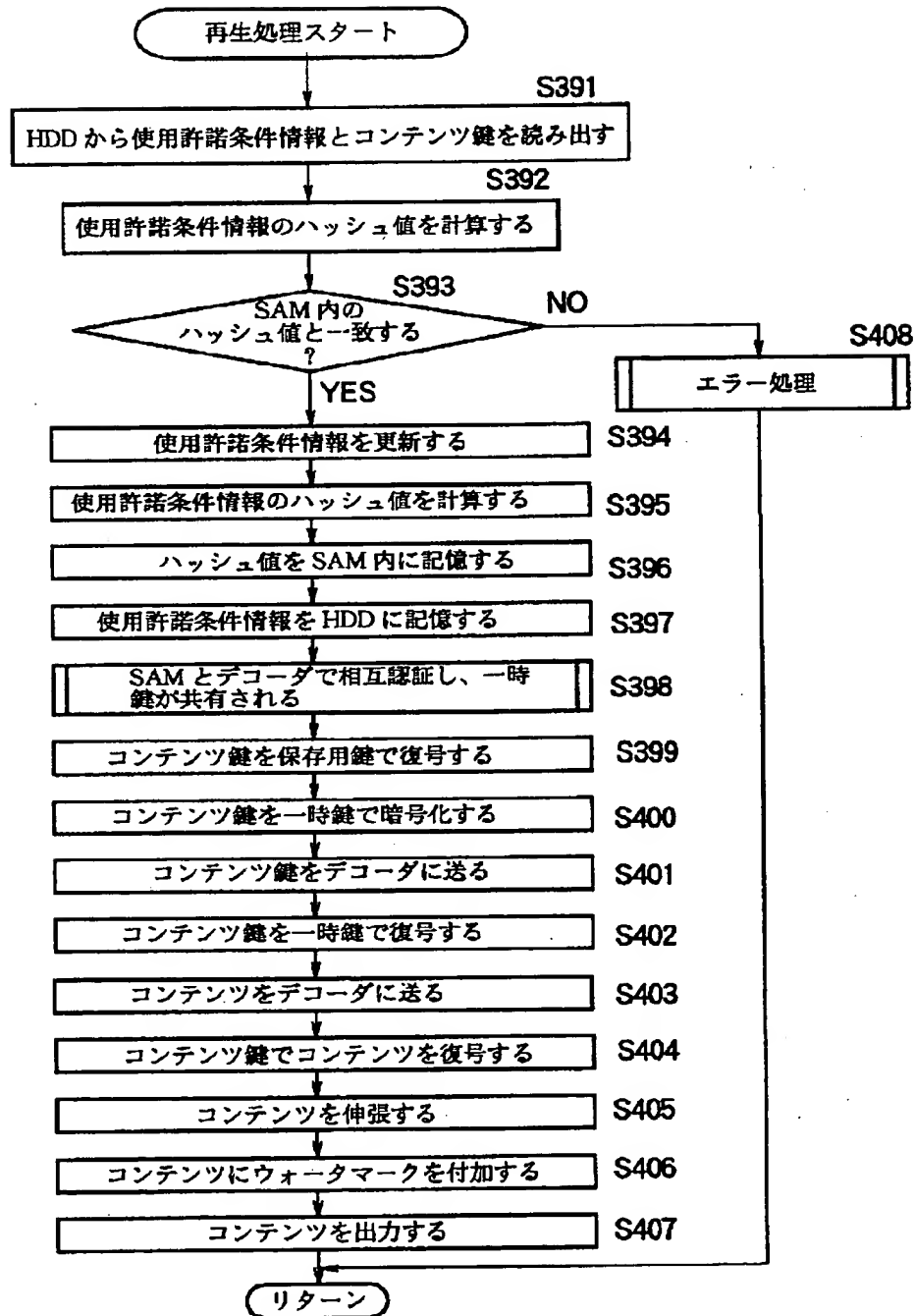
【図 5 4】



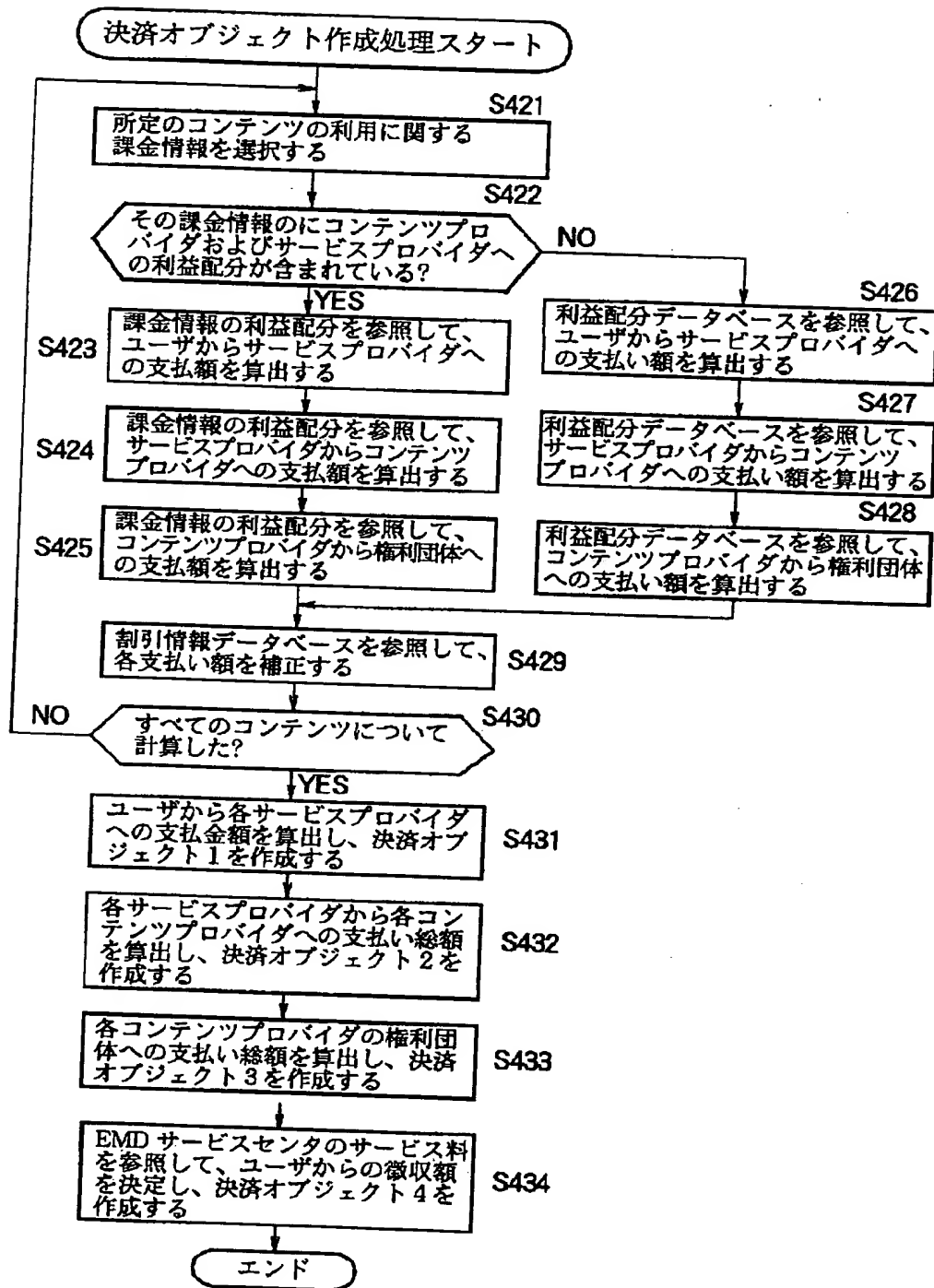
【図 55】



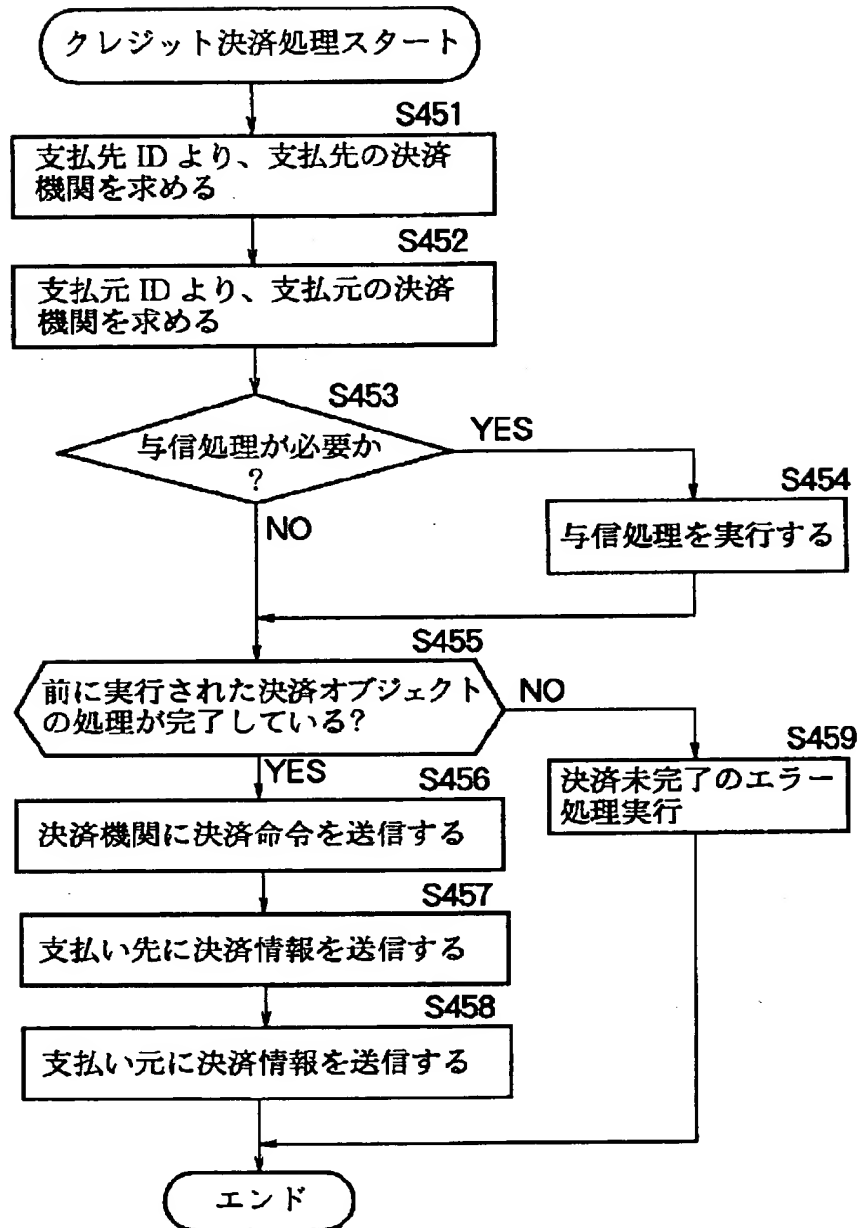
【図 56】



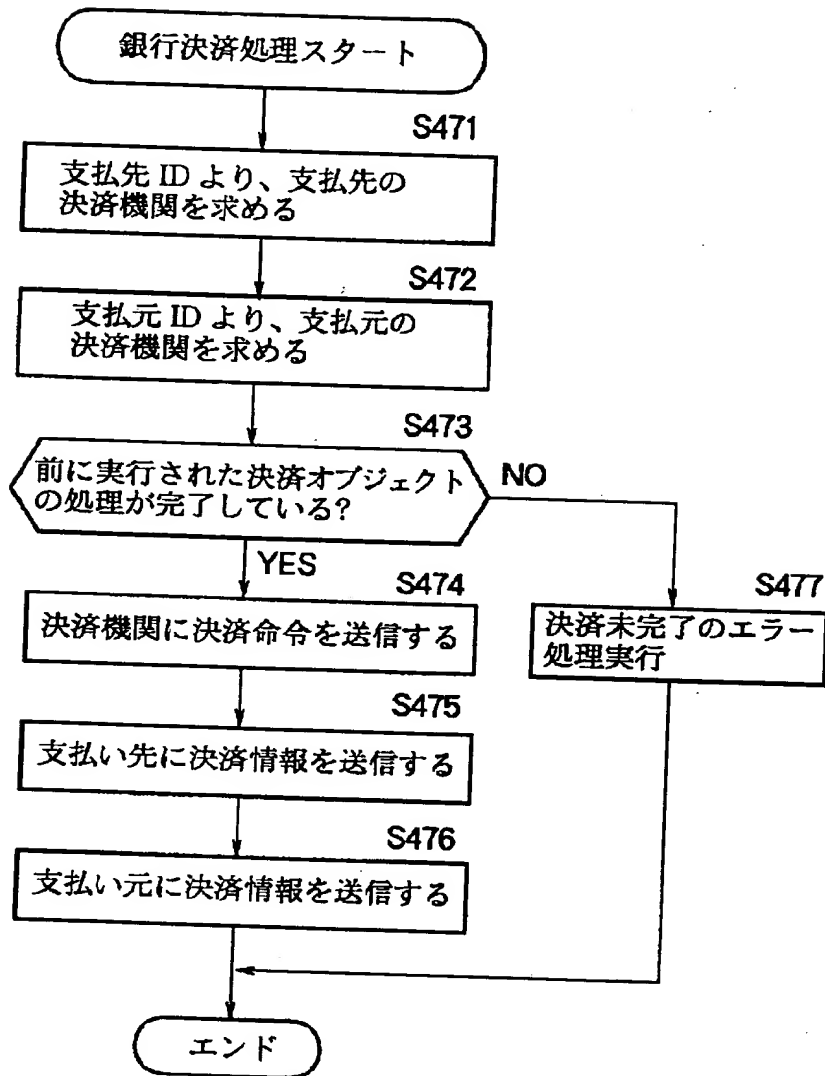
【図57】



【図 61】



【図 62】



フロントページの続き

(51) Int. Cl.

H04L 9/32

12/54

12/58

// H04M 15/00

識別記号

FI

H04M 15/00

H04L 9/00

11/20

テマコード (参考)

Z

675B

101Z

Fターム(参考) 5B049 AA05 BB11 BB46 CC31 CC36
CC39 EE02 EE03 FF06 FF09
GG04 GG07 GG10
5B089 GA11 GA21 GB03 HA01 JA40
KA15
5J104 AA07 KA01 KA05 MA02 PA07
PA10
5K025 AA05 BB10 CC01
5K030 HB08 HB21 HC01 KA01

THIS PAGE BLANK (USPTO)

Date of Laid-Open: April 28, 2000

[Title of the Invention]

INFORMATION PROCESSING APPARATUS, INFORMATION
PROCESSING METHOD, AND MEDIUM FOR PROVIDING THE SAME

[Abstract]

[Objective] To enable settlement processing and profit-calculation processing to be performed efficiently.

[Means for Solution] A profit-distribution section 16 stores data which specify information, and data which indicate an amount to be paid to each information provider for use of the information. The profit-distribution section 16 calculates the sum total of amounts to be paid to each information provider, on the basis of the stored data. A treasury section 20 instructs a settlement institute to perform settlement for each information provider, on the basis of profit gained by each information provider, which is calculated by the profit-distribution section 16.

[Claims]

[Claim 1] An information processing apparatus which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, characterized by comprising:

storage means for storing data which specify said information, and data which indicate an amount to be paid to

each of said information providers for use of said information;

calculation means for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storage means; and

settlement instruction means for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Claim 2] An information processing apparatus as described in claim 1, characterized in that said calculation means further calculates the sum total of amounts to be paid to said information providers.

[Claim 3] An information processing apparatus as described in claim 1, characterized in that said storage means further stores information regarding an amount to be paid to an organization which collects copy-right fees of said information;

said calculation means further calculates the sum total of amounts to be paid to said organization; and

said settlement instruction means further instructs said settlement institute to perform settlement for said organization.

[Claim 4] An information processing apparatus as described in claim 1, characterized in that said storage means further stores data regarding discounts of usage fees of information.

[Claim 5] An information processing apparatus as described

in claim 1, characterized in that said settlement instruction means stores information regarding a settlement institute for each of said information providers.

[Claim 6] An information processing method which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, characterized by comprising:

a storing step for storing data which specify said information, and data which indicate an amount to be paid to each of said information providers for use of said information;

a calculating step for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storing step; and

a settlement instructing step for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Claim 7] A provision medium for providing a computer-readable program to an information processing apparatus which collects, on behalf of information providers, usage fees from users of information provided by said information providers and distributes profits to said information providers, said program causing said information processing apparatus to execute processing which comprises:

a storing step for storing data which specify said

information, and data which indicate an amount to be paid to each of said information providers for use of said information;

a calculating step for calculating the sum total of amounts to be paid to each of said information providers, on the basis of data stored in said storing step; and

a settlement instructing step for instructing a settlement institute to perform settlement for each of said information providers, on the basis of profits gained by each of said information providers.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention relates to an information processing apparatus, an information processing method, and a medium for providing the same. More particularly, the present invention relates to an information processing apparatus, an information processing method, and a medium for providing the same, which collect, on behalf of information providers, usage fees from information users and distribute profits to the information providers.

[0002]

[Prior Art] There exists a system such that encrypted information such as music is transmitted to an information processing apparatus of a user whose has signed a predetermined agreement, and the user decrypts the information on the information processing apparatus and plays back the music or the like. The information provider can

transmit information to a plurality of information providers to thereby provide services.

[0003]

[Problems to be Solved by the Invention] The information provider must enter an agreement with each of a plurality of users and collect usage fees. In addition, settlement processing and profit-calculation processing are wasteful in many aspects.

[0004] In view of the foregoing, an object of the present invention is to perform the settlement processing and profit-calculation processing more efficiently.

[0005]

[Means for Solving the Problems] The information processing apparatus described in claim 1 is characterized by comprising: storage means for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use of the information; calculation means for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storage means; and settlement instruction means for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0006] The information processing method described in claim 6 is characterized by comprising: a storing step for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use

of the information; a calculating step for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storing step; and a settlement instructing step for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0007] The provision medium described in claim 7 is characterized by providing a computer-readable program which causes an information processing apparatus to execute processing comprising a storing step for storing data which specify the information, and data which indicate an amount to be paid to each of information providers for use of the information; a calculating step for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storing step; and a settlement instructing step for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0008] In the information processing apparatus described in claim 1, the information processing method described in claim 6, and the provision medium described in claim 7, data which specify information, and data which indicate an amount to be paid to each of information providers for use of the information are stored; the sum total of amounts to be paid to each of the information providers is calculated on the

basis of the stored data; and an instruction is issued to a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers.

[0009]

[Embodiment of the Invention] Hereinbelow, an embodiment of the present invention will be described. In order to show the correspondence between the individual means of the invention described in the Claims and elements in the embodiment described below, in the following description regarding the feature of the present invention, each means is followed by a corresponding element (however, mere example) in the embodiment, enclosed in parentheses. However, this description does not mean that the individual means is limited to the described element.

[0010] An information processing apparatus described in claim 1 comprises storage means (e.g., a profit-distribution section 16 shown in FIG. 2) for storing data which specify information, and data which indicate an amount to be paid to each of information providers for use of the information; calculation means (e.g., the profit-distribution section 16 shown in FIG. 2) for calculating the sum total of amounts to be paid to each of the information providers, on the basis of data stored in the storage means; and settlement instruction means (e.g., a treasury section 20 shown in FIG. 2) for instructing a settlement institute to perform settlement for each of the information providers, on the basis of profit

gained by each of the information providers.

[0011] FIG. 1 is a diagram used for explaining an EMD (Electronic Music Distribution) system to which the present invention is applied. In the system, content distributed to a user refers to digital data whose information is valuable in itself. In the following description, music data are used as an example. An EMD service center 1 transmits a distribution key Kd to a content provider 2, a user home network 5, etc. The EMD service center 1 receives from the user home network 5 charging information produced in accordance with use of content, calculates a usage fee, and distributes profit to the content provider 2 and a service provider 3.

[0012] The content provider 2 holds digitized content. The content provider 2 inserts a watermark (electronic watermark) into the content in order to prove that the content is owned by the content provider 2, compresses and encrypts the content, adds predetermined information to the encrypted content, and transmits it to the service provider 3.

[0013] The service provider 3 adds price information to the content supplied from the content provider 2 and transmits it to the user home network 5 via a network 4, which is formed of a dedicated cable network, the Internet, or a satellite.

[0014] The user home network 5 receives the content and the price information attached thereto from the service provider 3, uses the content through decryption and reproduction, and executes charging processing. Charging information obtained

by the charging process is transmitted to the EMD service center 1 when the user home network 5 obtains a distribution key Kd from the EMD service center 1.

[0015] FIG. 2 is a block diagram showing the functional configuration of the EMD service center 1. A service-provider management section 11 supplies to the service provider 3 information regarding profit distribution. Further, when information (handling policy) which is added to content from the content provider 2 is encrypted information, the service-provider management section 11 transmits a distribution key Kd to the service provider 3. A content-provider management section 12 transmits to the content provider 2 a distribution key Kd and information regarding profit distribution. A copyright management section 13 transmits to an organization which manages copyrights; e.g., JASRAC (Japanese Society for Rights of Authors, Composers and Publishers) information which shows a record of use of the content by the user home network 5. A key server 14 stores distributions keys Kd and supplies the distributions keys Kd to the content provider 2, the user home network 5, etc., via the content-provider management section 12 or a user management section 18. The user management section 18 inputs and stores in a historical-data management section 15 charging information, which is information showing a record of use of content by the user home network 5, price information corresponding to the content, and handling policy corresponding to the content.

[0016] An example in which distribution keys Kd are regularly transmitted from the EMD service center 1 to the content provider 2 and a receiver 51 (which will be described in relation to FIG. 10) which constitutes the user home network 5 will be described with reference to FIGS. 3 to 6. FIG. 3 is a diagram which shows distribution keys Kd held by the EMD service center 1, distribution keys Kd held by the content provider 2, and distribution keys Kd held by the receiver 51, in January, 1998, when the content provider 2 starts provision of content and the receiver 51 constituting the user home network 5 starts use of the content.

[0017] In the example of FIG. 3, each distribution key Kd can be used from the first day to the last day of the corresponding calendar month. For example, a distribution key Kd of version 1 having a value of "aaaaaaaa," which is a random number having a predetermined number of bits, can be used from January 1, 1998 to January 31, 1998 (that is, a content key Kco which is used for encrypting content which the service provider 3 distributes to the user home network 5 during the period from January 1, 1998 to January 31, 1998 is encrypted by use of the distribution key Kd of version 1).

A distribution key Kd of version 2 having a value of "bbbbbbbb," which is a random number having a predetermined number of bits, can be used from February 1, 1998 to February 28, 1998 (that is, a content key Kco which is used for encrypting content which the service provider 3 distributes to the user home network 5 during that period is encrypted by

use of the distribution key Kd of version 2). Similarly, a distribution key Kd of version 3 can be used in March, 1998; a distribution key Kd of version 4 can be used in April, 1998; a distribution key Kd of version 5 can be used in May, 1998; and a distribution key Kd of version 6 can be used in June, 1998.

[0018] Before the content provider 2 starts provision of content, the EMD service center 1 transmits to the content provider 2 six distribution keys Kd of version 1 to 6, which can be used in January, 1998 to June, 1998. The content provider 2 receives and stores the six distribution keys Kd. The reason why the content provider 2 stores the distribution keys Kd for six months is that before provision of the content, the content provider 2 requires a certain period for preparation of the content and encryption of a content key.

[0019] Before the receiver 51 starts use of the content, the EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 1 to 3 which can be used in January, 1998 to March, 1998. The receiver 51 receives and stores the three distribution keys Kd. The reason why the receiver 51 stores the distribution keys Kd for three months is to avoid a situation such that the user home network 5 cannot utilize the content even within an agreed period during which the content is available, due to problems such that the receiver 51 cannot be connected to the EMD service center 1, and to reduce the frequency of the receiver 51

being connected to the EMD service center 1 and load on the user home network 5.

[0020] During the period from January 1, 1998 to January 31, 1998, the distribution key Kd of version 1 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0021] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on February 1, 1998 will be described with reference to FIG. 4. The EMD service center 1 transmits to the content provider 2 six distribution keys Kd of versions 2 to 7, which can be used from February, 1998 to July, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 2 to 4, which can be used from February, 1998 to April, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1 without erasing it. This is to allow use, when an unexpected trouble occurs or a fraudulent activity is performed or discovered, of the distribution key Kd which was used in the past.

[0022] During the period from February 1, 1998 to February 28, 1998, the distribution key Kd of version 2 is used among

the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0023] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on March 1, 1998 will be described with reference to FIG.

5. The EMD service center 1 transmits to the content provider 2 six distribution keys Kd of versions 3 to 8, which can be used from March, 1998 to August, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 3 to 5, which can be used from March, 1998 to May, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1 and the distribution key Kd of version 2 without erasing them.

[0024] During the period from March 1, 1998 to March 31, 1998, the distribution key Kd of version 3 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0025] Transmission of distribution keys Kd from the EMD service center 1 to the content provider 2 and the receiver 51 on April 1, 1998 will be described with reference to FIG.

6. The EMD service center 1 transmits to the content

provider 2 six distribution keys Kd of versions 4 to 9, which can be used from April, 1998 to September, 1998. The content provider 2 receives the six distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 transmits to the receiver 51 three distribution keys Kd of versions 4 to 6, which can be used from April, 1998 to June, 1998. The receiver 51 receives the three distribution keys Kd and overwrites them on the previously stored distribution keys Kd to thereby store the new distribution keys Kd. The EMD service center 1 stores the distribution key Kd of version 1, the distribution key Kd of version 2, and the distribution key Kd of version 3 without erasing them.

[0026] During the period from April 1, 1998 to April 30, 1998, the distribution key Kd of version 4 is used among the EMD service center 1, the content provider 2, and the receiver 51, which constitutes the user home network 5.

[0027] As described above, since distribution keys Ks for future months are distributed in advance, the user can purchase the content even when the user does not access the center at all during a period of one or two months, and can receive a key by accessing the center at a convenient time.

[0028] The profit-distribution section 16 calculates profits of the EMD service center 1, the content provider 2, and the service provider 3, on the basis of the charging information, price information, and handling policy, which are supplied

from the historical-data management section 15. A mutual authentication section 17 executes mutual authentication, which will be described later, with the content provider 2, the service provider 3, and a predetermined apparatus of the user home network 5.

[0029] The user management section 18 has a user-registration database. When a registration request is issued from the apparatus of the user home network 5, the user management section 18 searches the user-registration database, and, on the basis of the contents of the record, performs processing for registering the apparatus or denying the registration. When the user home network 5 consists of a plurality of apparatuses which can be connected to the EMD service center 1, the user management section 18 designates an apparatus to be used for settlement, on the basis of results of judgment as to whether individual apparatuses can be registered. Further, the user management section 18 transmits to the predetermined apparatus of the user home network 5 a registration list which prescribes conditions of use of the content.

[0030] FIG. 7 shows an example of the user-registration database. A 64-bit ID (Identification Data) peculiar to each apparatus of the user home network 5 is recorded. Further, for each ID (i.e., for each apparatus having the corresponding ID), there is provided information indicating whether the apparatus can perform settlement processing, information indicating whether the apparatus can be

registered, and information indicating whether the apparatus can be connected to the EMD service center 1. The information indicating possibility of registration recorded in the user-registration database is updated at predetermined time intervals, on the basis of information regarding nonpayment of fees, fraudulent processing, etc., provided from the settlement institute (e.g., bank) or the service provider 3. When an apparatus having an ID which is recorded as being not registerable issues a registration request, the user management section 18 denies the registration. Subsequent to this, the apparatus cannot utilize contents of the system.

[0031] The information indicating possibility of settlement processing recorded in the user-registration database indicates whether that apparatus can effect settlement. In the case in which the user home network 5 consists of a plurality of apparatuses which can use content through reproduction or copying thereof, among the plurality of apparatuses, one apparatus which can effect settlement outputs to the EMD service center 1 the charging information, price information, and handling policy for all the apparatuses of the user home network 5 registered in the EMD service center 1. The information indicating possibility of connection with the EMD service center 1 recorded in the user-registration database indicates whether that apparatus can be connected to the EMD service center 1. An apparatus which is recorded as being unconnectable outputs charging

information, etc. to the EMD service center 1 via other apparatuses of the user home network 5.

[0032] The user management section 18 receives charging information, price information, and handling policy supplied from apparatuses of the user home network 5 and outputs them to the historical-data management section 15. Further, through predetermined processing (at predetermined timing), the user management section 18 supplies distribution keys Kd to the user home network 5.

[0033] A charge billing section 19 calculates a charge for the user, on the basis of charging information, price information, and handling policy supplied from the historical-data management section 15, and supplies calculation results to the treasury section 20. The treasury section 20 communicates with an unillustrated external bank or a like organization in order to perform settlement processing, on the basis of amounts of money to be paid to and usage fees to be collected from the user, the content provider 2, and the service provider 3. An auditor section 21 audits accuracy of the charging information, price information, and handling policy supplied from the apparatus of the user home network 5 (i.e., whether fraudulence is present therein).

[0034] FIG. 8 is a block diagram showing the functional configuration of the content provider 2. A content server 31 stores content to be supplied to users and supplies it to a watermark adding section 32. The watermark adding section 32

adds a watermark to the content supplied from the content server 31 and sends it to a compression section 33. The compression section 33 compresses the content supplied from the watermark adding section 32 in accordance with an ATRAC2 (Adaptive Transform Acoustic Coding 2) (Trademark) scheme or any other scheme and supplies the compressed content to an encryption section 34. The encryption section 34 encrypts the content compressed by the compression section 33 in accordance with a common key cryptosystem such as DES (Data Encryption Standard) and by use, as a key, of a random number supplied from a random-number generation section 35 (hereinafter, this random number will be referred to as a content key Kco), and outputs the result of the encryption to a secure container creation section 38.

[0035] The random-number generation section 35 outputs to the encryption section 34 and the encryption section 36 a random number having a predetermined number of bits and serving as a content key Kco. The encryption section 36 encrypts the content key Kco in accordance with a common key cryptosystem such as DES and by use of a distribution key Kd supplied from the EMD service center 1, and outputs the results of encryption to the secure container creation section 38.

[0036] DES is an encryption system which processes plain text while handling 64 bits as a single block. The processing of DES consists of a portion (data scrambling section) for scrambling plain text and converting it into

encrypted text, and a portion (key processing section) for generating from a common key a key (extended key) to be used in the data scrambling section. Since the entire algorithm of DES is opened to the public, here, the basic processing of the data scrambling section will be described briefly.

[0037] First, 64 bits of plain text are divided into upper 32 bits H_0 and lower 32 bits L_0 . A 48-bit extended key K_1 supplied from the key processing section and the lower 32 bits L_0 are used as inputs in order to calculate an output of an F-function in which the lower 32 bits L_0 have been scrambled. The F-function consists of "replacement" for replacing numerals in accordance with a predetermined rule and "transposition" for transposing bit positions in accordance with a predetermined rule. Subsequently, the upper 32 bits H_0 and the F-function output are subjected to exclusive-OR, and the result is used as L_1 . L_0 is used as H_1 .

[0038] On the basis of the upper 32 bits H_0 and the lower 32 bits L_0 , the above-described processing is repeated 16 times; and the thus-obtained upper 32 bits H_{16} and lower 32 bits L_{16} are output as encrypted text. Decryption is performed to inversely follow the above-described steps, while using the common key used in the encryption.

[0039] A policy storage section 37 stores a policy on handling of content, and outputs to the secure container creation section 38 a handling policy corresponding to content to be encrypted. The secure container creation section 38 creates a content-provider secure container and

supplies it to the service provider 3. The content-provider secure container includes encrypted content; an encrypted content key K_{co} ; a handling policy; a signature created from hash values of the encrypted content, the encrypted content key K_{co} , and the handling policy; and a certificate including a public key K_{pcp} of the content provider 2. Before receiving a distribution key K_d from the EMD service center 1, a mutual authentication section 39 mutually authenticates with the EMD service center 1. Further, before transmission of the content-provider secure container to the service provider 3, the mutual authentication section 39 mutually authenticates with the service provider 3.

[0040] Signature refers to data which are attached to data or a certificate, which will be described later, in order to enable check for tampering and perform author authentication. A hash value is obtained by use of a hash function and on the basis of data to be transmitted; and the thus-obtained hash value is encrypted by a private key of a public key cryptosystem.

[0041] The hash function and signature collation will be described. The hash function is a function which receives predetermined data to be transmitted, compresses the data into data having a predetermined bit length, and outputs the result as a hash value. The hash function has features such that an input is difficult to predict from a hash value (output), that when a certain bit of data input to the hash function changes, many bits of the hash value change, and

that finding input data having the same hash value is difficult.

[0042] A receiving person who has received a signature and data decrypts the signature by use of a public key of the public key cryptosystem to obtain a resultant value (hash value). Further, a hash value of the received data is calculated; and a judgment is made as to whether the calculated hash value is equal to the hash value obtained through decryption of the signature. When the hash value of the transmitted data is judged to be equal to the decrypted hash value, this means that the received data have not been subjected to tampering and have been transmitted from a transmitting person who holds a private key corresponding to the public key. Examples of the hash function for signature include MD4, MD5, and SHA-1.

[0043] Next, the public key cryptosystem will be described. In contrast to a common key cryptosystem in which the same key (common key) is used for encryption and decryption, in the public key cryptosystem, a key used for encryption differs from a key used for decryption. When the public key cryptosystem is employed, even when one of the keys is disclosed, the other can be kept secret. A key which may be opened to the public is called a public key; and a key which is kept secret is called a private key.

[0044] RSA (Rivest-Shamir-Adleman) cryptosystem, which is a typical example of the public key cryptosystem, will be described briefly. First, two sufficiently large prime

numbers p and q are obtained, and then a product n of p and q is obtained. The least common multiple L of $(p-1)$ and $(q-1)$ is calculated. Subsequently, a number e which is at least 3 but less than L and which shares no common factors with L (i.e., 1 is the only natural number by which both e and L can be divided evenly) is obtained.

[0045] Subsequently, a multiplicative inverse element d of e modulo L is obtained. That is, $ed=1 \bmod L$ holds among d , e , and L , and d can be calculated through the Euclidean algorithm. n and e are used as public keys; and p , q , and d are used as private keys.

[0046] An encrypted text C is calculated from a plain text M through processing of formula (1).

$$C = M^e \bmod n \quad (1)$$

[0048] The encrypted text C is decrypted to the plain text M through processing of formula (2).

$$M = C^d \bmod n \quad (2)$$

[0048] Although proof is omitted, the reason why a plain text can be converted to an encrypted text by the RSA cryptosystem and the encrypted text can be decrypted is based on Fermat's theorem, and formula (3) stands.

$$M = C^d = (M^e)^d = M^{ed} \bmod n \quad (3)$$

[0049] If the private keys p and q are known, the private key d can be calculated from the public key e . However, if the number of digits of the public key n is increased to a degree such that factorization of n in prime numbers is difficult from the viewpoint of calculation volume, even if the public

key n is known, the private key d cannot be calculated from the public key e , making decryption impossible. As described above, in the RSA cryptosystem, the key used for decryption is made different from the key used for encryption.

[0050] Further, the elliptic-curve cryptosystem, which is another example of the public key cryptosystem, will be described briefly. Assume that a certain point on an elliptic curve $y^2 = x^3 + ax + b$ is denoted by B . Addition of points on the elliptic curve is defined, and nB represents a result of n times of addition of B . Similarly, subtraction is defined. It has been proved that calculating n from B and nB is difficult. B and nB are used as public keys; and n is used as a private key. Encrypted texts $C1$ and $C2$ are calculated from a plain text M by use of a random number r and the public key, through processing represented by formulas (4) and (5).

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

[0051] The encrypted texts $C1$ and $C2$ are decrypted to the plain text M through processing of formula (6).

$$M = C1 - nC2 \quad (6)$$

[0052] Only a person who has the private key n can decrypt the encrypted texts. As described above, as in the case of the RSA cryptosystem, when the elliptic-curve cryptosystem is employed, the key used for decryption can be made different from the key used for encryption.

[0053] FIG. 9 is a block diagram showing the functional

structure of the service provider 3. A content server 41 stores encrypted content supplied from the content provider 2 and supplies it to a secure container creation section 44. A pricing section 42 creates price information on the basis of a handling policy corresponding to the content and supplies it to the secure container creation section 44. A policy storage section 43 stores the handling policy of the content supplied from the content provider 2 and supplies it to the secure container creation section 44. Before receiving a content-provider secure container from the content provider 2, a mutual authentication section 45 mutually authenticates with the content provider 2. Further, before transmission of a service-provider secure container to the user home network 5, the mutual authentication section 45 mutually authenticates with the user home network 5. When the content provider 2 supplies the handling policy after encryption with a distribution key K_d , the mutual authentication section 45 mutually authenticates with the EMD service center 1, before reception of the distribution key K_d from the EMD service center 1.

[0054] FIG. 10 is a block diagram showing the configuration of the user home network 5. The receiver 51 receives a service-provider secure container including content from the service provider 3 via the network 4; and decrypts, extends, and reproduces the content.

[0055] A communication section 61 communicates with the service provider 3 and the EMD service center 1 via the

network 4 to thereby receive information therefrom and transmit information thereto. A SAM (Secure Application Module) 62 mutually authenticates with the service provider 3 or the EMD service center 1; decrypts a cipher of the content or encrypts the content; and stores the distribution key K_d and other data. An extension section 63 decrypts the cipher of the content, extends it in accordance with the ATRAC2 scheme, and inserts a predetermined watermark into the content. An IC (Integrated Circuit)-card interface 64 converts the signal from the SAM 62 into a predetermined form and outputs the result to an IC card 55 attached to the receiver 51; and converts the signal from the IC card 55 into a predetermined form and outputs the result to the SAM 62.

[0056] The SAM 62—which mutually authenticates with the service provider 3 or the EMD service center 1, performs charging processing, decrypts and encrypts the content key K_{co} , and stores predetermined data such as information regarding conditions for permission of use (hereinafter referred to as "conditions-for-use information")—includes a mutual authentication module 71, a charging processing module 72, a storage module 73, and a decryption/encryption module 74. The SAM 62 is formed of a single chip IC dedicated for cipher processing which has a multilayer structure such that an internal memory cell is sandwiched between dummy layers of, for example, aluminum and has characteristics (tampering resistance) which make it difficult to illegally read data from the outside; such as a

narrow operable voltage range and a narrow operable frequency range.

[0057] The mutual authentication module 71 mutually authenticates with the service provider 3 or the EMD service center 1; and, if necessary, supplies a temporary key Ktemp (session key) to the decryption/encryption module 74. The charging processing module 72 generates charging information and conditions-for-use information, from the handling policy and price information (and handling control information in some cases) contained in the service-provider secure container received from the service provider 3; and outputs them to the storage module 73 or a HDD (Hard Disk Drive) 52. The storage module 73 stores various data such as the charging information and a distribution key Kd supplied from the charging processing module 72 or the decryption/encryption module 74. When any other function block performs predetermined processing, the storage module 73 supplies the distribution key Kd and other data to that block.

[0058] The decryption/encryption module 74 includes a decryption unit 91, a random-number generation unit 92, and an encryption unit 93. The decryption unit 91 decrypts an encrypted content key Kco with a distribution key Kd and outputs it to the encryption unit 93. The random-number generation unit 92 generates a random number having a predetermined number of digits and outputs the random number to the encryption unit 93 and the storage module 73 as a save

key Ksave. When the save key Ksave is already generated and stored, generation of the key is not required. The encryption unit 93 encrypts the decrypted content key Kco with the save key Ksave and outputs it to the HDD 52. When the content key Kco is transmitted to the extension section 62, the encryption unit 93 encrypts the content key Kco with the temporary key Ktemp.

[0059] The extension section 63—which decrypts and extends the content and adds a predetermined watermark to the content—includes a mutual authentication module 75, a decryption module 76, a decryption module 77, an extension module 78, and a watermark addition module 79. The mutual authentication module 75 mutually authenticates with the SAM 62 and outputs the temporary key Ktemp to the decryption module 76. The decryption module 76 decrypts the content key Kco—which was encrypted with the temporary key Ktemp—with the temporary key Ktemp and outputs it to the decryption module 77. The decryption module 77 decrypts the content stored in the HDD 52 with the content key Kco and outputs it to the extension module 78. The extension module 78 extends the decrypted content in accordance with ATRAC2 or any other scheme and outputs it to the watermark addition module 79. the watermark addition module 79 inserts into the content a predetermined watermark specifying the receiver 51 and outputs it to a recorder 53; and outputs the content to an unillustrated speaker to thereby reproduce music.

[0060] The HDD 52 records thereon the content supplied from

the service provider 3. The recorder 53—which records the content supplied from the service provider 3 on an attached optical disk (not shown) and reproduces the content—includes a record/reproduction section 65, an SAM 66, and an extension section 67. The record/reproduction section 65 includes an optical disk attached thereto and adapted to record the content on the optical disk and reproduce the content from the optical disk. The SAM 66 has the same function as that of the SAM 62, and therefore repeated description is omitted. The extension section 67 has the same function as that of the extension section 63, and therefore repeated description is omitted. An MD (Mini Disk; trademark) drive 54 records the content supplied from the service provider 3 on an attached MD (not shown) and reproduces the content from the MD.

[0061] The IC card 55 is attached to the receiver 51 and stores predetermined data such as an equipment ID and the distribution key Kd stored in the storage module 73. In an example case in which a user has purchased a new receiver 51 and uses it in place of the previous receiver 51, the user first stores in the IC card 55 predetermined data such as the distribution key Kd which are stored in the storage module 73 of the previous receiver 51. Next, the user attaches the IC card 55 to the new receiver 51 and operates the receiver 51 in order to register the new receiver 51 in the user management section 18 of the EMD service center 1. On the basis of the data (ID of the previous receiver 51, etc.)

stored in the IC card 55, the user management section 18 of the EMD service center 1 searches the database held in the user management section 18 to obtain data in relation to the user, such as the name of the user, and the number of a credit card used for payment of usage fees. On the basis of the data, the user management section 18 executes registration processing. Therefore, the user is not required to input data, which is cumbersome. The IC card 55 includes a mutual authentication module 80 and a storage module 81. The mutual authentication module 80 mutually authenticates with the SAM 62. The storage module 81 stores the data supplied from the SAM 62 via the IC-card interface 64 and outputs the stored data to the SAM 62.

[0062] FIG. 11 is a block diagram showing another configuration of the user home network 5. The receiver 51 and the recorder 53 in the present configuration do not have the extension sections 63 and 67 shown in FIG. 10. Instead, a decoder 56 connected to the recorder 53 provides the same function as that provided by the extension section 63 or 67. The remaining sections and modules have the same configurations as those in FIG. 10.

[0063] The decoder 56—which decrypts and extends the content and adds a watermark to the content—includes a mutual authentication module 101, a decryption module 102, a decryption module 103, an extension module 104, and a watermark addition module 105. The mutual authentication module 101 mutually authenticates with the SAM 62 or the SAM

66 and outputs the temporary key Ktemp to the decryption module 102. The decryption module 102 decrypts the content key Kco—which was encrypted with the temporary key Ktemp and is output from the SAM 62—with the temporary key Ktemp and outputs it to the decryption module 103. The decryption module 103 decrypts the content stored in the HDD 52 with the content key Kco and outputs it the extension module 104. The extension module 104 extends the decrypted content in accordance with ATRAC2 or any other scheme and outputs it to the watermark addition module 105. the watermark addition module 105 inserts into the content a predetermined watermark specifying the decoder 56 and outputs it to the recorder 53; and outputs the content to an unillustrated speaker to thereby reproduce music.

[0064] FIG. 12 is a diagram used for describing information which is exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The content provider 2 stores encrypted content, an encrypted content key Kco, a handling policy, and a signature in a content-provider secure container (details of which will be described with reference to FIG. 13); attaches a certificate of the content provider 2 (details of which will be described with reference to FIG. 14) to the content-provider secure container; and transmits the content-provider secure container to the service provider 3. Further, the content provider 2 transmits to the EMD service center 1 the handling policy and the signature to which the certificate of

the content provider 2 is attached.

[0065] The service provider 3 generates price information on the basis of the handling policy contained in the received content-provider secure container, and stores the encrypted content, the encrypted content key Kco, the handling policy, the price information, and the signature in a service-provider secure container (details of which will be described with reference to FIG. 15); attaches a certificate of the service provider 3 (details of which will be described with reference to FIG. 16) to the service-provider secure container; and transmits the service-provider secure container to the user home network 5. Further, the service provider 3 transmits to the EMD service center 1 the price information and the signature to which the certificate of the service provider 3 is attached.

[0066] The user home network 5 generates use-permission information from the handling policy contained in the received service-provider secure container, and uses the content in accordance with the use-permission information. When the content key Kco is decrypted in the user home network 5, charging information is generated. At a predetermined timing, the charging information is encrypted, and the handling policy and the signature are attached to the encrypted charging information, which is then transmitted to the EMD service center 1.

[0067] The EMD service center 1 calculates a usage fee on the basis of the charging information and the handling policy

and further calculates respective profits of the EMD service center 1, the content-provider secure container 2, and the service provider 3. Moreover, the EMD service center 1 compares the handling policy received from the content provider 2, the price information received from the service provider 3, and the charging information and the handling policy received from the user home network 5 in order to check (audit) whether illegal conduct such as tampering with the handling policy or illegal price increase has occurred in the service provider 3 or the user home network 5.

[0068] FIG. 13 is a diagram used for describing the content-provider secure container. The content-provider secure container includes content encrypted by use of a content key K_{co} ; the content key K_{co} encrypted by use of a distribution key K_d ; a handling policy; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key K_{co} ; the content key K_{co} encrypted by use of the distribution key K_d , and the handling policy in order to obtain a hash value, which is then encrypted by use of a private key K_{scp} of the content provider 2.

[0069] FIG. 14 is a diagram used for describing the certificate of the content provider 2. The certificate of the content provider 2 includes a version number of the certificate; a serial number of the certificate which an authentication office has allocated to the content provider 2; an algorithm and parameters used in the signature; the

name of the authentication office; a valid term of the certificate; the name of the content provider 2; the public key Kpcp of the content provider; and a signature. The signature is data which are obtained as follows. A hash function is applied to the version number of the certificate; the serial number of the certificate which the authentication office has allocated to the content provider 2; the algorithm and parameters used in the signature; the name of the authentication office; the valid term of the certificate; the name of the content provider 2; and the public key Kpcp of the content provider in order to obtain a hash value, which is then encrypted by use of a private key Ksca of the authentication office.

[0070] FIG. 15 is a diagram used for describing the service-provider secure container. The service-provider secure container includes the content encrypted by use of the content key Kco; the content key Kco encrypted by use of the distribution key Kd; the handling policy; price information; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, the handling policy, and the price information in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0071] FIG. 16 is a diagram used for describing the certificate of the service provider 3. The certificate of

the service provider 3 includes a version number of the certificate; a serial number of the certificate which an authentication office has allocated to the service provider 3; an algorithm and parameters used in the signature; the name of the authentication office; a valid term of the certificate; the name of the service provider 3; the public key K_{psp} of the service provider; and a signature. The signature is data which are obtained as follows. A hash function is applied to the version number of the certificate; the serial number of the certificate which the authentication office has allocated to the service provider 3; the algorithm and parameters used in the signature; the name of the authentication office; the valid term of the certificate; the name of the service provider 3; and the public key K_{psp} of the service provider in order to obtain a hash value, which is then encrypted by use of the private key K_{sca} of the authentication office.

[0072] FIG. 17 is a diagram showing a handling policy, price information, and conditions-for-use information. The content provider 2 has a handling policy for each piece of content, and the handling policy shows items which the user home network 5 can utilize. For example, the handling policy of FIG. 17(A) permits the user home network 5 to perform reproduction and multicopying of content but does not permit the user home network 5 to perform single copying of the content.

[0073] FIG. 18 is a diagram used for describing multicopying

and single copying. A user can perform single copying or multicopying when the user has purchased permission for using content whose copying is permitted under conditions-for-use information. Multicopying refers to making a plurality of copies. However, as shown in FIG. 18(A), the user cannot (is not permitted to) make a copy of a copy. Single copying refers to making a single copy. In the case of single copying as well, as shown in FIG. 18(B), the user cannot (is not permitted to) make a copy of a copy.

[0074] As shown in FIG. 17(B), the service provider 3 adds price information to the handling policy supplied from the content provider 2. For example, the price information shown in FIG. 17(B) indicates that usage fee for reproduction of the content is 150 yen and that usage fee for multicopying is 80 yen. Although not exemplified in FIG. 17, price information for single copying indicates usage fee for making a single copy, and in an example case in which the user performs copying three times, the user pays a fee three times that for single copying. Multicopying or single copying is permitted for only content for which copying is permitted under conditions-for-use information and for which the user has purchased permission for use.

[0075] When the user selects some of the usable items of the content (FIG. 17(B)) indicated by the handling policy supplied from the service provider 3, the user home network 5 stores conditions-for-use information (FIG. 17(C)) which indicates the item(s) selected by the user. For example, the

conditions-for-use information of FIG. 17(C) permits the user home network 5 to reproduce the content but does not permit the user home network 5 to perform single copying and multicopying.

[0076] FIG. 19 is a diagram used for describing a handling policy and price information. This example differs from the example shown in FIG. 17 in that the content provider 2 adds information regarding profit distribution to the handling policy, and the service provider 3 adds the information regarding profit distribution to the price information. In contrast to the example of FIG. 17, in the example of FIG. 19, information indicating that the content provider 2 can obtain a profit of 70 yen from a user's use in the form of reproduction of the content and a profit of 40 yen from a user's use in the form of multicopying is added (FIG. 19(A)). Further, profit-distribution information indicating that the service provider 3 can obtain a profit of 60 yen from a user's use in the form of reproduction of the content and a profit of 30 yen from a user's use in the form of multicopying is added (FIG. 19(B)). An amount of money (e.g., 20 yen) obtained through subtraction of a profit (e.g., 70 yen) of the content provider 2 and a profit (e.g., 60 yen) of the service provider 3 from a price (e.g., 150 yen) is a profit of the EMD service center 1. The EMD service center 1 obtains charging information (FIG. 19(C)) which shows the use of the content by the user home network 5. The EMD service center 1 further obtains a handling policy, profit-

distribution ratios, and price information via the user home network 5, to thereby calculate the respective profits of the content provider 2, the service provider 3, and the EMD service center 1).

[0077] FIG. 20 is a diagram used for describing a handling policy, price information, and conditions-for-use information for the case in which a plurality of manners of reproduction of the content are set. In the example of FIG. 20(A), the service provider 3 sets the handling policy and price information to reflect a plurality of manners of reproduction of the content; i.e., limitless reproduction, reproduction within a limited number of times (5 times in this example), and reproduction within a limited period (until December 31, 1998 in this case). When a user uses the content while selecting the reproduction which is limited to 5 times, "5" is recorded, as a maximum number of times, in the conditions-for-use information of the user home network 5 as shown in FIG. 20(B) in a state in which the user has not yet reproduced the content after receipt thereof. This value indicating the maximum number of times is decremented every time the content is reproduced (used) in the user home network 5. For example, after the content is reproduced three times, the value is changed to "2" as shown in FIG. 20(C). When the value of the number limit becomes "0," the user home network 5 becomes unable to further reproduce and use the content.

[0078] FIG. 21 is a diagram showing another example of

information exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The example of FIG. 21 differs from the example of FIG. 12 in that the service provider 3 creates handling control information on the basis of the handling policy received from the content provider 2. The handling control information is stored in the service-provider secure container together with the content and other data and is then transmitted to the user home network 5 and the EMD service center 1. Further, the handling control information is transmitted from the user home network 5 to the EMD service center 1 together with charging information and the handling policy.

[0079] FIG. 22 is a diagram used for describing a service-provider secure container used in the example of FIG. 21. The service-provider secure container includes a content encrypted by use of a content key Kco; the content key Kco encrypted by use of a distribution key Kd; a handling policy; handling control information; price information; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key Kco, the content key Kco encrypted by use of the distribution key Kd, the handling policy, the handling control information, and the price information in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0080] FIG. 23 shows the details of the handling policy,

handling control information, and conditions-for-use information in the example of FIG. 21. In the example of FIG. 23, the handling policy of the content provider 2 (FIG. 23(A)) does not have a form such that simple addition of price information enables referral to price information through comparison between the handling policy and the price information. In view of the foregoing, on the basis of the handling policy, there is produced handling control information having a form which enables referral to price information through comparison between the handling policy and the price information; and the price information is added to the handling control information, which is then transmitted to the user home network 5 (FIG. 23(B)). The user home network 5 produces conditions-for-use information from the received information (FIG. 23 (C)). As compared to the case of FIG. 12, the content provider 2 in FIG. 23 has an advantage in that the handling policy that the content provider 2 is required to record is of a further reduced amount of data.

[0081] FIG. 24 is a diagram showing another example of content and information accompanying the content, which are exchanged among the EMD service center 1, the content provider 2, the service provider 3, and the user home network 5. The example of FIG. 24 differs from the example of FIG. 21 in that in the example of FIG. 24 a handling policy, handling control information, price information, and charging information are encrypted by means of a public cryptosystem

and are then transmitted. As compared to the case of FIG. 21, the system in FIG. 24 has enhanced safety against attack from outside the system.

[0082] FIG. 25 is a diagram used for describing a content-provider secure container used in the example of FIG. 24. The content-provider secure container includes content encrypted by use of a content key K_{co} ; the content key K_{co} encrypted by use of a distribution key K_d ; a handling policy encrypted by use of the distribution key K_d ; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key K_{co} , the content key K_{co} encrypted by use of the distribution key K_d , and the handling policy encrypted by use of the distribution key K_d in order to obtain a hash value, which is then encrypted by use of a private key K_{scp} of the content provider 2.

[0083] FIG. 26 is a diagram used for describing a service-provider secure container used in the example of FIG. 24. The service-provider secure container includes the content encrypted by use of the content key K_{co} ; the content key K_{co} encrypted by use of the distribution key K_d ; the handling policy encrypted by use of the distribution key K_d ; handling control information encrypted by use of the distribution key K_d ; price information encrypted by use of the distribution key K_d ; and a signature. The signature is data which are obtained as follows. A hash function is applied to the content encrypted by use of the content key K_{co} , the content

key Kco encrypted by use of the distribution key Kd, the handling policy encrypted by use of the distribution key Kd, the handling control information encrypted by use of the distribution key Kd, and the price information encrypted by use of the distribution key Kd in order to obtain a hash value, which is then encrypted by use of a private key Kssp of the service provider 3.

[0084] FIG. 27 is a diagram used for describing another operation of the EMD service center 1 for collecting data necessary for settlement processing, from the content provider 2, the service provider 3, and the user home network 5. The content provider 2 transmits to the EMD service center 1 content-provider registration data consisting of the name of the content provider 2, a content ID, a profit of a proprietor organization corresponding to the content ID, and the number of a bank account of the content provider 2; and the content-provider management section 12 of the EMD service center 1 receives the content-provider registration data. Upon reception of the content-provider registration data, the content-provider management section 12 of the EMD service center 1 generates a content-provider ID and registers the content-provider registration data, together with the content-provider ID, into a profit-distribution database. Further, the content-provider management section 12 transmits the content-provider ID to the content provider 2. The content provider 2 receives and stores the content-provider ID.

[0085] The service provider 3 transmits to the EMD service center 1 service-provider registration data consisting of the name of the service provider 3, a content ID, and the number of a bank account of the service provider 3; and the service-provider management section 11 of the EMD service center 1 receives the service-provider registration data. Upon reception of the service-provider registration data, the service-provider management section 11 of the EMD service center 1 generates a service-provider ID and transmits the service-provider ID to the service provider 3. The service provider 3 receives and stores the content-provider ID.

[0086] The user home network 5 transmits to the EMD service center 1 user registration data consisting of the name of a user and the number of a bank account of the user; and the user management section 18 of the EMD service center 1 receives the user registration data. Upon reception of the user registration data, the user management section 18 of the EMD service center 1 generates a user ID, stores the user registration data together with the user ID, and transmits the user ID to the user home network 5. The user home network 5 receives and stores the user ID.

[0087] FIG. 28 is a diagram showing an example of the profit-distribution database. Distribution of profit to the proprietor organization corresponding to each content ID is stored in the profit-distribution database. The distribution of profit to the proprietor organization corresponding to a content ID indicates a ratio of distribution to the

proprietor organization of a profit which is produced when content corresponding to the content ID is utilized by the user.

[0088] In the example profit-distribution database shown in FIG. 28, when content whose content ID is 1 is provided from the service provider 3 to the user, 10% of the profit produced from utilization of the content by the user is distributed to the proprietor organization. Similarly, when content whose content ID is 2 is used by the user, 20% of the profit produced from utilization of the content by the user is distributed to the proprietor organization.

[0089] FIG. 29 shows a content-fee discount table stored in the profit-distribution section 16 of the EMD service center 1. The content-fee discount table stores discount rates of usage fees to be paid by users for each combination of a content ID and a content-provider ID. The discount table is designed to store other information items such as periods during which individual discount rates are applied.

[0090] A usage fee for content whose content ID is 1 and which is supplied from a content provider 2 whose content-provider ID is 1 is discounted at a rate of 0.02 during a period from September, 1998 to December, 1998. A usage fee for content whose content ID is 2 and which is supplied from a content provider 2 whose content-provider ID is 1 is discounted at a rate of 0.03. A usage fee for content which has a content ID other than 1 and 2 and which is supplied from a content provider 2 whose content-provider ID is 1 is

discounted at a rate of 0.01. A usage fee for content whose content ID is 3 and which is supplied from a content provider 2 whose content-provider ID is 2 is discounted at a rate of 0.05. A usage fee for content whose content ID is 1 and which is supplied from a service provider 3 whose service-provider ID is 1 is discounted at a rate of 0.03. A usage fee for content whose content ID is 4 and which is supplied from a service provider 3 whose service-provider ID is 2 is discounted at a rate of 0.01.

[0091] FIG. 30 shows a user's usage-fee table stored in the charge billing section 19 of the EMD service center 1. The user's usage-fee table stores a usage fee which the user pays to the EMD service center 1. A monthly basic charge in the user's usage-fee table indicates a fixed usage fee which the user pays to the EMD service center 1 each month. An adjustment amount indicates a discount rate that is applied to the monthly basic charge during a predetermined special period and a discount rate that is applied to the monthly basic charge when the usage fee, including usage fees of contents, exceeds a predetermined amount.

[0092] In the example user's usage-fee table shown in FIG. 30, the monthly basic charge is 1000 yen; and the monthly basic charge is discounted by 10% during a period from August, 1998 to September, 1998. Further, when the usage fee, including usage fees for contents, exceeds 3000 yen, the monthly basic charge is discounted by 5%.

[0093] A usage fee for content is calculated from the

profit-distribution database or charging information; a discount amount is subtracted from the thus-calculated content usage fee; and the fee for use of the EMD service center 1 is added thereto, whereby a usage fee to be paid by a corresponding user is calculated.

[0094] FIG. 31 shows an operation of the EMD service center 1 when the EMD service center 1 receives charging information from the user home network 5. After performing mutual authentication with the user home network 5, the user management section 18 converts the temporary key Ktemp to a shared temporary key Ktemp, encrypts a distribution key Kd from the key server 14 by use of the shared temporary key Ktemp, and transmits it to the user home network 5. After decrypting the received distribution key Kd by use of the shared temporary key Ktemp, the user home network 5 updates the distribution key Kd if necessary. Further, the user home network 5 encrypts charging information, a handling policy, and other data by use of the shared temporary key Ktemp and transmits them to the EMD service center 1. The user management section 18 receives the encrypted data. After decrypting the received charging information, handling policy, and other data by use of the shared temporary key Ktemp, the user management section 18 transmits them to the historical-data management section 15 and the charge billing section 19. When the historical-data management section 15 judges that settlement must be executed, the historical-data management section 15 transmits the received charging information to the

profit-distribution section 16 and transmits the received charging information, handling policy, and other data to the charge billing section 19. With reference to the profit-distribution database and the discount table, the profit-distribution section 16 calculates amounts to be charged to and amounts to be paid to the content provider 2, the service provider 3, and the EMD service center 1, through processing which will be described later with reference to FIG. 57. The charge billing section 19 calculates an amount to be charged to each user on the basis of the user's usage-fee table, and transmits the information to the treasury section 20. The treasury section 20 communicates with an unillustrated outside bank or the like to thereby perform settlement processing. At this time, when information indicating user's nonpayment of fee or any other fact is present, such information is transmitted from the charge billing section 19 and the user management section 18 and is referred to during subsequent processing for user registration or processing for transmission of distribution keys Kd.

[0095] FIG. 32 shows an operation of the EMD service center 1 for profit distribution processing. The historical-data management section 15 transmits to the profit-distribution section 16 charging information indicative of past use of content by a user, a handling policy, and price data. On the basis of these information items, the profit-distribution section 16 calculates respective profits of the content provider 2, the service provider 3, and the EMD service

center 1 and transmits the results of calculation to the service-provider management section 11, the content-provider management section 12, the treasury section 20, and the copyright management section 13. The treasury section 20 communicates with the unillustrated outside bank or the like to thereby perform setting processing. The service-provider management section 11 transmits to the service provider 3 information regarding the profit of the service provider 3. The content-provider management section 12 transmits to the content provider 2 information regarding the profit of the content provider 2. The auditor section 21 audits accuracy of the charging information, price information, and handling policy supplied from the apparatus of the user home network 5.

[0096] FIG. 33 shows an operation of the EMD service center 1 for transmitting to JASRAC information regarding past use of content by a user. The historical-data management section 15 transmits to the copyright management section 13 and the profit-distribution section 16 charging information indicative of past use of the content by the user. With reference to the profit-distribution database and the discount table, the profit-distribution section 16 calculates an amount to be charged to and an amount to be paid to JASRAC, and transmits that information to the treasury section 20, through processing which will be described later with reference to FIG. 57. The treasury section 20 communicates with the unillustrated outside bank or the like to thereby perform settlement processing. The copyright management

section 13 transmits to JASRAC a record of use of the content by the user.

[0097] Next, processing performed by the EMD system will be described. FIG. 34 is a flowchart used for describing the processing performed by the system in order to distribute and reproduce content. In step S11, the content-provider management section 12 of the EMD service center 1 transmits distribution keys Kd to the content provider 2; and the content provider 2 receives them. The details of this processing will be described later with reference to the flowchart of FIG. 36. In step S12, a user operates an apparatus (e.g., the receiver 51 of FIG. 10) of the user home network 5 in order to register the apparatus in the user management section 18 of the EMD service center 1. The details of this registration processing will be described later with reference to the flowchart of FIG. 40. In step S13, as shown in FIGS. 37 to 39, the user management section 18 of the EMD service center 1 transmits distribution keys Kd to the apparatus of the user home network 5 after mutual authentication. The user home network 5 receives the keys. The details of this processing will be described later with reference to the flowchart of FIG. 48.

[0098] In step S14, the secure container creation section 38 of the content provider 2 transmits a content-provider secure container to the service provider 3. The details of this transmission processing will be described later with reference to the flowchart of FIG. 50. In step S15, in

response to a request from the user home network 5, the secure container creation section 44 of the service provider 3 transmits a service-provider secure container to the user home network 5 via the network 4. The details of this transmission processing will be described later with reference to the flowchart of FIG. 52. In step S16, the charging processing module 72 of the user home network 5 performs charging processing. The details of this charging processing will be described later with reference to the flowchart of FIG. 54. In step S17, the user reproduces the content on the apparatus of the user home network 5. The details of this reproduction processing will be described later with reference to the flowchart of FIG. 55.

[0099] Processing performed by the content provider 2 in order to encrypt and transmit a handling policy is shown by the flowchart of FIG. 35. In step S21, the content-provider management section 12 of the EMD service center 1 transmits distribution keys K_d to the content provider 2. In step S22, the service-provider management section 11 of the EMD service center 1 transmits distribution keys K_d to the service provider 3. Processing performed in subsequent steps S23 to S28 is similar to that performed in steps S12 to S17 of FIG. 24, and hence repeated description is omitted.

[0100] FIG. 36 is a flowchart used for describing the details of processing corresponds to step S11 of FIG. 34 and step S21 of FIG. 35. In this processing, the EMD service center 1 transmits distribution keys K_d to the content

provider 2, and the content provider 2 receives them. In step S31, the mutual authentication section 17 of the EMD service center 1 mutually authenticates with the mutual authentication section 39 of the content provider 2. The details of this mutual authentication processing will be described later with reference to the flowchart of FIG. 37. When, through the mutual authentication processing, the content provider 2 has been confirmed to be an authorized provider, in step S32 the encryption section 34 and the encryption section 36 of the content provider 2 receive the distribution keys K_d transmitted from the content-provider management section 12 of the EMD service center 1. In step S33, the encryption section 34 of the content provider 2 stores the received distribution keys K_d .

[0101] As described above, the content provider 2 receives the distribution keys K_d from the EMD service center 1. Similarly, in an example case in which processing of the flowchart shown in FIG. 35 is performed, not only the content provider 2 but also the service provider 3 receives the distribution keys K_d from the EMD service center 1, through processing similar to that shown in FIG. 36.

[0102] Next, the mutual authentication processing, which is performed in step S31 of FIG. 36 in order to confirm that so-called disguise is not present, will be described with reference to three example cases; i.e., a case in which a single common key is used (FIG. 37), a case in which two common keys are used (FIG. 38), and a case in which a public

key cryptosystem is used (FIG. 39).

[0103] FIG. 37 is a flowchart showing mutual authentication operation which the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 perform while using a single common key of DES, which is a common key cryptosystem. In step S41, the mutual authentication section 39 of the content provider 2 generates a random number R1 of 64 bits (the random-number generation section 35 may generate the random number). In step S42, the mutual authentication section 39 of the content provider 2 encrypts the random number R1 by use of a previously stored common key Kc, in accordance with the DES (the encryption section 36 may perform this encryption). In step S43, the mutual authentication section 39 of the content provider 2 transmits the encrypted random number R1 to the mutual authentication section 17 of the EMD service center 1.

[0104] In step S44, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R1 by use of the previously stored common key Kc. In step S45, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 32 bits. In step S46, the mutual authentication section 17 of the EMD service center 1 replaces lower 32 bits of the decrypted 64-bit random number R1 with the random number R2 to thereby generate a concatenated number $R1_H || R2$. Here, $R1_H$ represents the upper bits of R1, and $A || B$ represents a concatenation of

A and B (where B having m bits is joined to a lower portion of A having n bits to thereby obtain a number of (n+m) bits). In step S47, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number $R1_H || R2$ by use of the common key Kc in accordance with the DES. In step S48, the mutual authentication section 17 of the EMD service center 1 transmits the encrypted $R1_H || R2$ to the content provider 2.

[0105] In step S49, the mutual authentication section 39 of the content provider 2 decrypts the received $R1_H || R2$ by use of the common key Kc . In step S50, the mutual authentication section 39 of the content provider 2 investigates the upper 32 bits $R1_H$ of the decrypted concatenated number $R1_H || R2$ and authenticates that the EMD service center 1 is an authorized center, when the upper 32 bits $R1_H$ coincide with the upper 32 bits $R1_H$ of the random number $R1$ generated in step S41. When the generated random number $R1_H$ does not coincide with the received $R1_H$, the processing is ended. When they coincide with each other, in step S51, the mutual authentication section 39 of the content provider 2 generates a random number $R3$ of 32 bits. In step S52, the mutual authentication section 39 of the content provider 2 generates a concatenated number $R2 || R3$, while using the received and decrypted 32-bit random number as an upper half of the concatenated number and the generated random number $R3$ as a lower half of the concatenated number. In step S53, the mutual authentication section 39 of the content provider 2 encrypts the

concatenated number $R2 || R3$ by use of the common key K_s in accordance with the DES. In step S54, the mutual authentication section 39 of the content provider 2 transmits the encrypted concatenation number $R2 || R3$ to the mutual authentication section 17 of the EMD service center 1.

[0106] In step S55, the mutual authentication section 17 of the EMD service center 1 decrypts the received concatenated number $R2 || R3$ by use of the common key K_c . In step S56, the mutual authentication section 17 of the EMD service center 1 investigates the upper 32 bits of the decrypted concatenated number $R2 || R3$ and authenticates that the content provider 2 is an authorized provider, when the upper 32 bits coincide with the random number $R2$. When the upper 32 bits do not coincide with the random number $R2$, the content provider 2 is judged to be an unauthorized provider, and the processing is ended.

[0107] FIG. 38 is a flowchart showing mutual authentication operation which the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 perform while using two common keys K_{c1} and K_{c2} in accordance with DES, which is a common key cryptosystem. In step S61, the mutual authentication section 39 of the content provider 2 generates a random number $R1$ of 64 bits. In step S62, the mutual authentication section 39 of the content provider 2 encrypts the random number $R1$ by use of a previously stored common key K_{c1} in accordance with the DES. In step S63, the mutual

authentication section 39 of the content provider 2 transmits the encrypted random number R1 to the EMD service center 1.

[0108] In step S64, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R1 by use of the previously stored common key Kc1. In step S65, the mutual authentication section 17 of the EMD service center 1 encrypts the random number R1 by use of a previously stored common key Kc2. In step S66, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 64 bits.. In step S67, the mutual authentication section 17 of the EMD service center 1 encrypts the random number R2 by use of the common key Kc2. In step S68, the mutual authentication section 17 of the EMD service center 1 transmits the encrypted random numbers R1 and R2 to the mutual authentication section 39 of the content provider 2.

[0109] In step S69, the mutual authentication section 39 of the content provider 2 decrypts the received random numbers R1 and R2 by use of the previously stored common key Kc2. In step S70, the mutual authentication section 39 of the content provider 2 investigates the decrypted random number R1 and authenticates that the EMD service center 1 is an authorized center, when the decrypted random number R1 coincides with the random number R1 generated in step S61 (random number R1 before being subjected to encryption). When they do not coincide with each other, the EMD service center 1 is judged to be an unauthorized center, and the processing is ended.

In step S71, the mutual authentication section 39 of the content provider 2 encrypts with the common key Kc1 the random number R2 obtained through decryption. In step S72, the mutual authentication section 39 of the content provider 2 transmits the encrypted random number R2 to the EMD service center 1.

[0110] In step S73, the mutual authentication section 17 of the EMD service center 1 decrypts the received random number R2 by use of the common key Kc1. In step S74, the mutual authentication section 17 of the EMD service center 1 authenticates that the content provider 2 is an authorized provider, when the decrypted random number R2 coincides with the random number R2 generated in step S66 (random number R2 before being subjected to encryption). When they do not coincide with each other, the content provider 2 is judged to be an unauthorized provider, and the processing is ended.

[0111] FIG. 39 is a flowchart showing mutual authentication operation performed by the mutual authentication section 39 of the content provider 2 and the mutual authentication section 17 of the EMD service center 1 while using an elliptic-curve cryptosystem of 160-bit length, which is a public key cryptosystem. In step S81, the mutual authentication section 39 of the content provider 2 generates a random number R1 of 64 bits. In step S82, the mutual authentication section 39 of the content provider 2 transmits to the mutual authentication section 17 of the EMD service center 1 the random number R1 and a certificate which has

been obtained in advance from an authentication office and which includes a public key Kpcp of the content provider 2. [0112] In step S83, the mutual authentication section 17 of the EMD service center 1 decrypts the signature of the received certificate (having been encrypted by use of a private key Ksca of the authentication office) by use of a public key Kpca of the authentication office which has been obtained in advance, to thereby extract hash values of the public key Kpcp of the content provider 2 and the name of the content provider 2. The mutual authentication section 17 of the EMD service center 1 extracts the public key Kpcp of the content provider 2 and the name of the content provider 2, which are stored in the form of plain text. If the certificate is a proper one issued by the authentication office, decryption of the signature of the certificate is possible; and the hash values of the public key Kpcp of the content provider 2 and the name of the content provider 2 coincide with hash values obtained as a result of applying a hash function to the public key Kpcp of the content provider 2 and the name of the content provider 2 which are stored in the certificate in the form of plain text. Thus, the public key Kpcp is authenticated to be an authorized one and not to have been subjected to tampering. When the signature cannot be decrypted or when the hash values extracted from the signature do not coincide with those obtained by use of a hash function, this means that the public key Kpcp is not an authorized public key, or the content provider 2 is not an

authorized provider. In this case, the processing is ended.

[0113] When a proper authentication result is obtained, in step S84, the mutual authentication section 17 of the EMD service center 1 generates a random number R2 of 64 bits. In step S85, the mutual authentication section 17 of the EMD service center 1 generates a concatenated number $R1 || R2$ of the random numbers R1 and R2. In step S86, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number $R1 || R2$ by use of the private key Ksesc of the EMD service center 1. In step S87, the mutual authentication section 17 of the EMD service center 1 encrypts the concatenated number $R1 || R2$ by use of the public key Kpcp of the content provider 2 obtained in step S83. In step S88, the mutual authentication section 17 of the EMD service center 1 transmits to the mutual authentication section 39 of the content provider 2 the concatenated number $R1 || R2$ encrypted by use of the private key Ksesc, the concatenated number $R1 || R2$ encrypted by use of the public key Kpcp, and a certificate including the public key Kpesc of the EMD service center 1 (which has been obtained in advance from the authentication office).

[0114] In step S89, the mutual authentication section 39 of the content provider 2 decrypts the signature of the received certificate by use of the previously obtained public key Kpca of the authentication office; and when the signature is correct, the mutual authentication section 39 extracts the public key Kpesc from the certificate. Since the processing

in this case is similar to that in step S83, its repeated description is omitted. In step S90, the mutual authentication section 39 of the content provider 2 decrypts the concatenated number $R1||R2$ having been encrypted by use of the private key K_{sesc} of the EMD service center 1, by use of the public key K_{pesc} obtained in step S89. In step S91, the mutual authentication section 39 of the content provider 2 decrypts the concatenated number $R1||R2$ having been encrypted by use of the public key K_{pcp} of the content provider 2, by use of the private key K_{scp} of the content provider 2. In step S92, the mutual authentication section 39 of the content provider 2 compares the concatenated number $R1||R2$ decrypted in step S90 and that decrypted in step S91. When they coincide with each other, the mutual authentication section 39 authenticates that the EMD service center 1 is an authorized one. When they do not coincide with each other, the mutual authentication section 39 judges that the EMD service center 1 is not an authorized one, and ends the processing.

[0115] When a proper authentication result is obtained, in step S93, the mutual authentication section 39 of the content provider 2 generates a random number $R3$ of 64 bits. In step S94, the mutual authentication section 39 of the content provider 2 generates a concatenated number $R2||R3$ of the generated random number $R3$ and the random number $R2$ obtained in step S90. In step S95, the mutual authentication section 39 of the content provider 2 encrypts the concatenated number

R2||R3 by use of the public key Kpesc obtained in step S89. In step 96, the mutual authentication section 39 of the content provider 2 transmits the encrypted, concatenated number R2||R3 to the mutual authentication section 17 of the EMD service center 1.

[0116] In step S97, the mutual authentication section 17 of the EMD service center 1 decrypts the encrypted, concatenated number R2||R3 by use of the private key Ksesc of the EMD service center 1. In step S98, the mutual authentication section 17 of the EMD service center 1 authenticates that the content provider 2 is an authorized provider, when the decrypted random number R2 coincides with the random number R2 generated in step S84 (random number R2 before being subjected to encryption). When they do not coincide with each other, the mutual authentication section 17 judges that the content provider 2 is not an authorized provider, and ends the processing.

[0117] As described above, the mutual authentication section 17 of the EMD service center 1 and the mutual authentication section 39 of the content provider 2 authenticate each other. Random numbers used in the mutual authentication are each used as a temporary key Ktemp, which is effective only in processing subsequent to the mutual authentication.

[0118] FIG. 40 is a flowchart used for describing the details of processing corresponding to step S12 of FIG. 34 and step S23 of FIG. 35. In this processing, the receiver 51 performs registration in the user management section 18 of the EMD.

service center 1. In step S101, on the basis of output from the IC-card interface 64, the SAM 62 of the receiver 51 judges whether the IC card 55 for backup is attached to the receiver 51. When the IC card 55 for backup has been attached to the receiver 51 (e.g., a case in which the receiver 51 is replaced with a new receiver 51, and the data contained in the previous receiver 51 are stored in the IC card 55 in order to transfer the data of the previous receiver 51 to the new receiver 51), the SAM 62 proceeds to step S102 in order to read backup data stored in the IC card 55. The details of this processing will be described later with reference to the flowchart of FIG. 45. Needless to say, in order to enable this read processing, the backup data must be stored in the IC card 55 beforehand. This backup processing will be described later with reference to FIG. 43.

[0119] When in step S101 the IC card 55 is judged not to be attached to the receiver 51, the SAM 62 skips step S102 and proceeds to step S103. In step S103, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1, and the SAM 62 transmits a certificate to the user management section 18 of the EMD service center 1. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, its repeated description is omitted here. The certificate that the SAM 62 transmits to the user management section 18 of the EMD service center 1 in step S103 includes data shown in FIG. 41.

The certificate transmitted by the SAM 62 has a configuration substantially the same as that of the content provider 2 shown in FIG. 14. However, the certificate transmitted by the SAM 62 further contains data indicating whether the SAM 62 belongs to another SAM. In step S104, the SAM 62 transmits, via the communication section 61 to the user management section 18 of the EMD service center 1, information regarding a settlement institution such as a bank of the user, which information has been encrypted by use of the temporary key Ktemp.

[0120] In step S105, on the basis of the received ID of the SAM 62, the user management section 18 of the EMD service center 1 searches the user-registration database shown in FIG. 7. In step S106, the user management section 18 of the EMD service center 1 judges whether a SAM 62 having the received ID can be registered. When the SAM 62 can be registered, the user management section 18 proceeds to step S107 in order to judge whether registration of the SAM 62 is new. When it is judged in step S107 that the registration of the SAM 62 is not a new registration, the user management section 18 proceeds to step S108.

[0121] In step S108, the user management section 18 of the EMD service center 1 executes processing for update registration in order to search the user-registration data base on the basis of the received Id and to make a registration list. This registration list has a configuration as shown in FIG. 42. For each of the IDs of

SAMs of apparatuses, this registration list includes a registration denial flag indicating whether the user management section 18 of the EMD service center 1 has denied registration; a status flag which is used in a case in which an SAM depends on another SAM and which shows conditions for use of a content key Kco; a condition flag indicating whether the SAM depends on another SAM; and a signature. The signature has been obtained through encryption, with the private key Ksesc of the EMD service center 1, of a hash value generated through application of a hash function to the registration denial flag, the status flag, and the condition flag.

[0122] The SAM of each apparatus has a 64-bit ID unique to the apparatus (indicated by hexadecimal numbers in FIG. 42). When the registration denial flag is "1," this indicates that the user management section 18 of the EMD service center 1 has registered an apparatus having a corresponding ID. When the registration denial flag is "0," this indicates that the user management section 18 of the EMD service center 1 has denied registration of an apparatus having a corresponding ID.

[0123] When the MSB (Most Significant Bit) of the status flag is "1," this indicates that a child apparatus having a corresponding ID (e.g., the recorder 53) can receive a content key Kco from a parent apparatus (e.g., the receiver 51) on which the child apparatus depends. When the MSB of the status flag is "0," this indicates that a child apparatus having a corresponding ID cannot receive a content key Kco

from a parent apparatus on which the child apparatus depends. When the second bit of the status flag as counted from the MSB is "1," this indicates that a child apparatus having a corresponding ID can receive from a parent apparatus a content key Kco encrypted by use of a save key Ksave of the parent apparatus. When the third bit of the status flag as counted from the MSB is "1," this indicates that a child apparatus having a corresponding ID can receive from a parent apparatus a content key Kco encrypted by use of a distribution key Kd. When the LSB (Least Significant Bit) of the status flag is "1," this indicates that a parent apparatus on which a child apparatus having a corresponding ID depends purchases a content key Kco encrypted by use of a distribution key Kd, encrypts the content key Kco by use of a temporary key Ktemp, and passes the encrypted content key Kco to the child apparatus.

[0124] When the condition flag is "0," this indicates that an apparatus having a corresponding ID can communicate directly with the user management section 18 of the EMD service center 1 (i.e., this indicates that the apparatus having a corresponding ID is a parent apparatus such as the receiver 51). When the condition flag is "1," this indicates that an apparatus having a corresponding ID cannot communicate directly with the user management section 18 of the EMD service center 1 (i.e., this indicates that the apparatus having a corresponding ID is a child apparatus such as the recorder 53). When the condition flag is "0," the

status flag is set to "0000" at all times.

[0125] In step S109, the user management section 18 of the EMD service center 1 transmits to the SAM 62 of the receiver 51 a distribution key Kd which has been supplied from the key server 14 and encrypted by use of a temporary key Ktemp supplied from the mutual authentication section 17. In step S110, the SAM 62 of the receiver 51 decrypts the received distribution key Kd by use of the temporary key Ktemp and stores it in the storage module 73.

[0126] In step S111, the user management section 18 of the EMD service center 1 transmits to the SAM 62 of the receiver 51 the registration list encrypted by use of the temporary key Ktemp. In step S112, the SAM 62 of the receiver 51 decrypts the received registration list by use of the temporary key Ktemp and stores it in the storage module 73. Subsequently, the processing is ended.

[0127] When it is judged in step S107 that the registration of the SAM 62 is a new registration, the user management section 18 of the EMD service center 1 proceeds to step S114 to perform processing for new registration and produce a registration list. Subsequently, the user management section 18 proceeds to step S109.

[0128] When it is judged in step S106 that registration of a SAM having the received ID is impossible, the user management section 18 of the EMD service center 1 proceeds to step S113 to produce a registration list for registration denial. Subsequently, the user management section 18 proceeds to step

S111.

[0129] In the above-described manner, the receiver 51 is registered in the EMD service center 1.

[0130] Next, with reference to the flowchart of FIG. 43, there will be described the details of processing for storing in the IC card 55 predetermined data, such as a distribution key, which are stored in the storage module 73 of the receiver 51 having been used up to the present. In step S121, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S122, the random-number generation unit 92 of the SAM 62 generates a random number used as a backup key K_{ic} . In step S123, the encryption unit 93 of the SAM 62 encrypts the ID number of the SAM, the save key K_{save} , and the ID of the HDD 52, which are stored in the storage module 73, by use of the backup key K_{ic} . In step S124, the encryption unit 93 of the SAM 62 encrypts the backup key K_{ic} by use of the public key K_{pesc} of the EMD service center 1 (the SAM 62 has already obtained the public key K_{pesc} of the EMD service center 1 during authentication processing performed with the EMD service center 1 (step S89 in FIG. 39)). In step S125, the SAM 62 of the receiver 51 transmits, via the IC-card interface 64 to the IC card 55, the encrypted ID number of the SAM, the encrypted save key K_{save} , the encrypted ID of the HDD 52, and the encrypted

backup key Kic, to thereby store them in the storage module 81.

[0131] As described above, the ID number of the SAM, the save key Ksave, and the ID of the HDD 52, which are stored in the storage module 73 of the SAM 62, are encrypted by use of the backup key Kic, and stored in the storage module 81 of the IC card 55, together with the backup key Kic, which is encrypted by use of the public key Kpesc of the EMD service center 1.

[0132] With reference to the flowchart of FIG. 44, there will be described the details of other processing for storing in the IC card 55 predetermined data, such as a distribution key, which are stored in the storage module 73 of the receiver 51 having been used up to the present. In step S131, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication module 80 of the IC card 55. In step S132, the encryption unit 93 of the SAM 62 encrypts the ID number of the SAM, the save key Ksave, and the ID of the HDD 52, which are stored in the storage module 73, by use of the public key Kpesc of the EMD service center 1. In step S133, the SAM 62 of the receiver 51 transmits, via the IC-card interface 64 to the IC card 55, the encrypted ID number of the SAM, the encrypted save key Ksave, and the encrypted ID of the HDD 52, to thereby store them in the storage module 81.

[0133] The processing shown in FIG. 44, which is simpler than that shown in FIG. 43, enables the ID number of the SAM,

the save key Ksave, and the ID of the HDD 52 to be stored in the storage module 81 of the IC card 55 after being encrypted by use of the public key Kpesc of the EMD service center 1.

[0134] As described above, the backup data stored in the IC card 55 are read into the new receiver 51 by the processing in step S102 of FIG. 40. FIG. 45 is a flowchart used for describing processing for reading the backup data which have been stored in the IC card 55 by the processing shown in FIG. 43. In step 141, the mutual authentication module 71 of the SAM 62 of the new receiver 51 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0135] In step S142, the SAM 62 reads via the IC-card interface 64 from the storage module 81 data which was stored in the storage module 73 of the previous receiver 51 and encrypted by use of the backup key Kic (backup data of the ID number of the SAM, the save key Ksave, and the ID of the HDD 52), and the backup key Kic encrypted by use of the public key Kpesc of the EMD service center 1. In step S143, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S144, the SAM 62

transmits, via the communication section to the user management section 18 of the EMD service center 1, the data of the storage module 73 encrypted by use of the backup key Kic, as well as the backup key Kic encrypted by use of the public key Kpesc of the EMD service center 1.

[0136] In step S145, the user management section 18 of the EMD service center 1 decrypts the received backup key Kic by use of the private key Ksesc of the EMD service center 1. In step S146, the user management section 18 of the EMD service center 1 decrypts the received backup data by use of the backup key Kic. In step S147, the user management section 18 of the EMD service center 1 encrypts the decrypted backup data by use of the temporary key Ktemp supplied from the mutual authentication section 17. In step S148, the user management section 18 of the EMD service center 1 transmits to the communication section 61 of the user home network 51 the backup data encrypted by use of the temporary key Ktemp.

[0137] In step S149, the communication section 61 of the user home network 51 transmits to the SAM 62 the data received from the user management section 18 of the EMD service center 1. The SAM 62 decrypts the data and then stores them in the storage module 73. In step S150, the user management section 18 of the EMD service center 1 modifies the data in the user-registration database (FIG. 7) corresponding to the ID of the SAM 62 of the previous apparatus from which data was transferred to the IC card 55, such that the modified data indicate un-registerable.

[0138] As described above, the new receiver 51 reads the backup data from the IC card 55.

[0139] With reference to the flowchart shown in FIG. 46, there will be described processing for reading the backup data which have been stored in the IC card 55 by the processing shown in FIG. 44. In step S161, the mutual authentication module 71 of the SAM 62 of the new receiver 51 mutually authenticates with the mutual authentication module 80 of the IC card 55. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S162, the SAM 62 reads via the IC-card interface 64 data which was stored in the storage module 73 of the previous receiver 51 and encrypted by use of the public key Kpesc of the EMD service center 1 (backup data of the ID number of the SAM, the save key Ksave, and the ID of the HDD 52).

[0140] In step S163, the mutual authentication module 71 of the SAM 62 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S164, the SAM 62 transmits, via the communication section 61 to the user management section 18 of the EMD service center 1, the data of the storage module 73 encrypted by use of the public key Kpesc of the EMD service center 1.

[0141] In step S165, the user management section 18 of the

EMD service center 1 decrypts the data of the storage module 73 by use of the private key Ksesc of the EMD service center 1. In step S166, the user management section 18 of the EMD service center 1 encrypts the decrypted backup data by use of the temporary key Ktemp supplied from the mutual authentication section 17. In step S167, the user management section 18 of the EMD service center 1 transmits to the communication section 61 of the user home network 51 the backup data encrypted by use of the temporary key Ktemp. [0142] In step S168, the communication section 61 of the receiver 51 transmits to the SAM 62 the data received from the user management section 18 of the EMD service center 1. The SAM 62 decrypts the data and then stores them in the storage module 73. In step S169, the user management section 18 of the EMD service center 1 modifies the data in the user-registration database (FIG. 7) corresponding to the ID of the SAM 62 of the previous apparatus from which data was transferred to the IC card 55, such that the modified data indicate un-registerable.

[0143] As described above, when the backup is performed by use of the processing shown in FIG. 44, the new receiver 51 reads the backup data from the IC card 55 through the processing shown in FIG. 46.

[0144] When the receiver 51 registers itself (when the receiver 51 perform processing corresponding to step S12 of FIG. 34), the receiver 51 performs the processing shown in the flowchart of FIG. 40. When the receiver 51 registers the

recorder 53 depending on the receiver 51 in the EMD service center 1, the receiver 51 performs the processing shown in the flowchart of FIG. 47. In step S181, the SAM 62 of the receiver 51 writes the ID of the recorder 53 into the registration list stored in the storage module 73. In step S182, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0145] In step S183, on the basis of the ID of the receiver 51 (the ID of the SAM 62 contained in the certificate of the SAM 62 shown in FIG. 41), the user management section 18 of the EMD service center 1 searches the user-registration database and judges whether the receiver 51 is un-registerable. When the receiver 51 is judged not to be un-registerable, the processing proceeds to step S184. In step 184, the SAM 62 of the receiver 51 encrypts, by use of the temporary key Kd, the version of the distribution key Kd, charging information (stored by the processing in step S337 of the flowchart shown in FIG. 54, which will be described later), and the registration list, which are stored in the storage module 73. Further, the SAM 62 encrypts the handling policy stored in the HDD 52 by use of the temporary key Kd. Subsequently, the SAM 62 transmits via the communication section 61 to the user management section 18 of the EMD service center 1 the version of the distribution key Kd, the

charging information, and the registration list, which are stored in the storage module 73, as well as the handling policy stored in the HDD 52. In step S185, the user management section 18 of the EMD service center 1 decrypts the received data and processes the charging information. Subsequently, the user management section 18 updates the data portion (e.g., the registration denial flag and the status flag) which relates to the recorder 53 and which is contained in the registration list received from the receiver 51. The user management section 18 then attaches to the updated registration list a signature corresponding to the data corresponding to the receiver 51.

[0146] In step S186, the user management section 18 of the EMD service center 1 judges whether the version of the distribution key Kd which the receiver 51 holds is the latest. When the version of the distribution key Kd held by the receiver 51 is judged to be the latest, in step S187, the user management section 18 transmits to the receiver 51 the updated registration list and a charging-information receipt message, which have been encrypted by use of the temporary key Kd. The receiver 51 receives the updated registration list and the charging-information receipt message, decrypts them, and stores them. In step S188, the receiver 51 erases the charging information stored in the storage module 73, and replaces the stored registration list with the registration list received from the user management section 18 of the EMD service center 1 in step S187. Subsequently, the processing

proceeds to step S191.

[0147] When it is judged in step S186 that the version of the distribution key Kd held by the receiver 51 is not the latest, in step S189, the user management section 18 of the EMD service center 1 transmits to the receiver 51 a distribution key of the latest version, the updated registration list, and the charging-information receipt message, which have been encrypted by use of the temporary key Kd. The receiver 51 receives the distribution key of the latest version, the updated registration list, and the charging information receipt message, decrypts them, and stores them. In step S190, the receiver 51 erases the charging information stored in the storage module 73, replaces the stored registration list with the registration list received from the user management section 18 of the EMD service center 1 in step S189, and replaces the previous distribution key Kd with the distribution key of the latest version. Subsequently, the processing proceeds to step S191.

[0148] In step S191, with reference to the updated registration list, the SAM 62 of the receiver 51 judges whether the recorder 53 is un-registerable. When the recorder 53 is judged not to be un-registerable, in step S192, the receiver 51 and the recorder 53 mutually authenticate and share the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S193, the receiver 51 transmits to the

recorder 53 a registration completion message and the distribution key Kd, which have been encrypted by use of the temporary key Kd. The recorder 53 receives the registration completion message and the distribution key Kd, and decrypts them. In step S194, the recorder 53 updates the distribution key Kd, after which the processing ends.

[0149] The processing ends when it is judged in step S183 that the receiver 51 is un-registerable, or when it is judged in step S191 that the recorder 53 is un-registerable.

[0150] As described above, the recorder 53 depending on the receiver 51 is registered in the EMD service center 1 via the receiver 51.

[0151] FIG. 48 is a flowchart showing the details of the processing which is performed in step S13 of FIG. 34 in order to enable the receiver 51 to receive a distribution key Kd which is transmitted from the EMD service center 1 to the receiver 51. In step S201, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S202, the SAM 62 of the receiver 51 transmits a certificate to the user management section 18 of the EMD service center 1; and the user management section 18 of the EMD service center 1 receives the certificate. Since the processing in steps S203 to S210 is the same as that in steps S183 to S190 of FIG. 47,

repeated descriptions are omitted here.

[0152] As described above, the receiver 51 receives a distribution key Kd from the user management section 18 of the EMD service center 1 and transmits charging information of the receiver 51 to the user management section 18 of the EMD service center 1.

[0153] Next, with reference to the flowchart of FIG. 49, there will be described the details of the processing which enables the recorder 53 depending on the receiver 51 to receive a distribution key Kd (when the status flag shown in FIG. 42 has a value indicating that the recorder 53 is permitted to receive a distribution key Kd). In step S221, the mutual authentication module 71 of the receiver 51 and an unillustrated mutual authentication module of the recorder 53 mutually authenticate. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here.

[0154] In step S222, the receiver 51 judges whether the data of the recorder 53 are included in the registration list stored in the storage module 73 of the receiver 51. When it is judged that the data of the recorder 53 are included in the registration list stored in the storage module 73 of the receiver 51, in step S223, the receiver 51 judges whether the recorder 53 is un-registerable, with reference to the registration list stored in the storage module 73. When it is judged in step S223 that the recorder 53 is not un-registerable, in step S224, the SAM 66 of the recorder 53

encrypts, by use of the temporary key Ktemp, the version of the distribution key Kd stored in the internal storage module (which has been received from the receiver 51 in step S235 of FIG. 49, which will be described later) and charging information (which has been stored through processing corresponding step S337 of the processing corresponding to FIG. 54, which will be described later). Subsequently, the SAM 66 of the recorder 53 sends them to the SAM 62 of the receiver 51. The SAM 62 of the receiver 51 receives and decrypts the version of the distribution key Kd and the charging information.

[0155] In step S225, the mutual authentication module 71 of the receiver 51 mutually authenticates with the mutual authentication section 17 of the EMD service center 1 via the communication section 61. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S226, on the basis of the ID of the receiver 51, the user management section 18 of the EMD service center 1 searches the user-registration database and judges whether the receiver 51 is un-registerable. When the receiver 51 is judged not to be un-registerable, processing proceeds to step S227. In step 227, the SAM 62 of the receiver 51 encrypts, by use of the temporary key Kd, the version of the distribution key Kd, the charging information, and the registration list, which are stored in the storage module 73. Further, the SAM 62 encrypts the handling policy stored in

the HDD 52 and the charging information of the recorder 53 by use of the temporary key Kd. Subsequently, the SAM 62 transmits these data to the user management section 18 of the EMD service center 1 via the communication section 61. In step S228, the user management section 18 of the EMD service center 1 decrypts the received data and processes the charging information. Subsequently, the user management section 18 updates the data portion (e.g., the registration denial flag and the status flag) which relates to the recorder 53 and which is contained in the registration list received from the receiver 51, as has been described in relation to FIG. 42. The user management section 18 then attaches to the updated registration list a signature corresponding to the data corresponding to the receiver 51.

[0156] Since the processing in steps S229 to S234 is the same as that in steps S186 to S191 of FIG. 47, repeated description is omitted here.

[0157] In step S234, with reference to the updated registration list, the SAM 62 of the receiver 51 judges whether the recorder 53 is un-registerable. When the recorder 53 is judged not to be un-registerable, in step S235, the receiver 51 transmits to the recorder 53 a charging-information receipt message and the distribution key Kd, which have been encrypted by use of the temporary key Kd. The recorder 53 receives the charging-information receipt message and the distribution key Kd, and decrypts them. In step S236, the SAM 66 of the recorder 53 erases the charging

information stored in the internal storage module, and replaces the stored distribution key Kd with the distribution key Kd of the latest version.

[0158] When it is judged in step S222 that the data of the recorder 53 are not included in the registration list stored in the storage module 73 of the receiver 51, in step S237, the processing shown in FIG. 47 for registering the recorder 53 is executed. Processing then proceeds to step S224.

[0159] The processing ends when it is judged in step S223 that the recorder 53 is un-registerable, when it is judged in step S226 that the receiver 51 is un-registerable, or when it is judged in step S234 that the recorder 53 is un-registerable.

[0160] As described above, the recorder 53 depending on the receiver 51 receives the distribution key Kd via the receiver 51.

[0161] Next, with reference to the flowchart of FIG. 50, there will be described the processing which corresponds to step S14 of FIG. 34 and which enables the content provider 2 to transmit a content-provider secure container to the service provider 3. In step S251, the watermark adding section 32 of the content provider 2 inserts into content supplied from the content server 31 a predetermined watermark indicating the content provider 2, and sends it to the compression section 33. In step S252, the compression section 33 of the content provider 2 compresses the content in which the watermark has been inserted, in accordance with

ATRAC2 or any other scheme and supplies the compressed content to the encryption section 34. In step S253, the random-number generation section 35 generates a random number which is used as a content key Kco, and outputs it to the encryption section 34. In step S254, the encryption section 34 of the content provider 2 encrypts the content—into which the watermark has been inserted and which has been compressed, by use of the content key Kco and in accordance with a predetermined scheme such as DES.

[0162] In step S255, the encryption section 36 encrypts the content key Kco in accordance with a predetermined scheme such as DES and by use of the distribution key Kd which has been supplied from the EMD service center 1 through the processing in step S11 of FIG. 34. In step S256, the secure container creation section 38 of the content provider 2 applies a hash function to the encrypted content, the encrypted content key Kco, and the handling policy supplied from the policy storage section 37, in order to obtain a hash value, and then encrypts it by use of a private key Kscp of the content provider 2. Thus, a signature as shown in FIG. 13 is created. In step S257, the secure container creation section 38 of the content provider 2 creates a content-provider secure container as shown in FIG. 13, which includes the encrypted content, the encrypted content key Kco, and the handling policy supplied from the policy storage section 37, as well as the signature generated in step S256.

[0163] In step S258, the mutual authentication section 39 of

the content provider 2 mutually authenticates with the mutual authentication section 45 of the service provider 3. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S259, the secure container creation section 38 of the content provider 2 attaches to the content-provider secure container a certificate issued by the authentication office in advance and then transmits it to the service provider 3. Subsequently, the secure container creation section 38 ends the processing.

[0164] In the above-described manner, the content provider 2 transmits a content-provider secure container to the service provider 3.

[0165] Next, with reference to the flowchart of FIG. 51, there will be described the details of other processing which enables the content provider 2 to transmit a content-provider secure container to the service provider 3, wherein not only the content key K_{co} but also the handling policy is encrypted by use of the distribution key K_d . Since the processing in steps S271 to S274 is the same as that in steps S251 to S254 of FIG. 50, repeated description is omitted here. In step S275, the encryption section 36 of the content provider 2 encrypts the content key K_{co} and the handling policy supplied from the policy storage section 73, in accordance with a predetermined scheme such as DES and by use of the distribution key K_d which has been supplied from the EMD service center 1 through the processing in step S21 of FIG.

35.

[0166] In step S276, the secure container creation section 38 of the content provider 2 applies a hash function to the encrypted content, the encrypted content key Kco, and the encrypted handling policy in order to obtain a hash value, and then encrypts it by use of a private key Kscp of the content provider 2. Thus, a signature as shown in FIG. 25 is created. In step S277, the secure container creation section 38 of the content provider 2 creates a content-provider secure container as shown in FIG. 25, which includes the encrypted content, the encrypted content key Kco, and the encrypted handling policy, as well as the signature. The processing in step S278 is the same as that in step S258 of FIG. 50, and the processing in step S279 is the same as that in step S259 of FIG. 50. Therefore, repeated descriptions are omitted.

[0167] In the above-described manner, the content provider 2 transmits to the service provider 3 a content-provider secure container containing the encrypted handling policy.

[0168] Next, with reference to the flowchart of FIG. 52, there will be described the details of the processing which corresponds to step S15 of FIG. 34 and which enables the service provider 3 to transmit a service-provider secure container to the receiver 51. In step S291, the pricing section 42 of the service provider 3 checks the signature contained in the certificate which is attached to the content-provider secure container transmitted from the secure

container creation section 38 of the content provider 2. When the certificate has not been subjected to tampering, the pricing section 42 extracts the public key Kpcp of the content provider 2. Since the processing for checking the signature of the certificate is the same as that in step S83, repeated description is omitted here.

[0169] In step S292, the pricing section 42 of the service provider 3 decrypts, by use of the public key Kpcp of the content provider 2, the signature of the content-provider secure container transmitted from the secure container creation section 38 of the content provider 2, to thereby obtain a hash value. Subsequently, the pricing section 42 confirms that the thus-obtained hash value coincides with the hash value which is obtained through application of the hash function to the encrypted content, the encrypted content key Kco, and the handling policy, thereby confirming that the content-provider secure container has not been subjected to tampering. When it is found that the content-provider secure container has been subjected to tampering, the pricing section 42 ends the processing.

[0170] When the content-provider secure container has not been subjected to tampering, in step S293, the pricing section 42 of the service provider 3 extracts the handling policy from the content-provider secure container. In step S294, on the basis of the handling policy, the pricing section 42 of the service provider 3 produces price information, which has been described in relation to FIG. 17.

In step S295, the secure container creation section 44 of the service provider 3 produces a service-provider secure container as shown in FIG. 15. The service-provider secure container includes an encrypted content, an encrypted content key K_{co} , a handling policy, and price information, and a signature which is a value obtained through encryption, by use of its own private key K_{ssp} , of a hash value which is obtained through application of a hash function to the encrypted content, the encrypted content key K_{co} , the handling policy, and the price information.

[0171] In step S296, the mutual authentication section 45 of the service provider 3 mutually authenticates with the mutual authentication module 71 of the receiver 51. Since this mutual authentication is the same as that described with reference to FIGS. 37 to 39, repeated description is omitted here. In step S297, the secure container creation section 44 of the service provider 3 transmits to the communication section 61 of the receiver 51 the service-provider secure container to which the certificate has been attached. Subsequently, the secure container creation section 44 ends the processing.

[0172] In the above-described manner, the service provider 3 transmits a service-provider secure container to the receiver 51.

[0173] Next, with reference to the flowchart of FIG. 53, there will be described the details of the processing which enables the service provider 3 to transmit a service-provider

secure container to the receiver 51, wherein the handling policy is encrypted by use of the distribution key Kd in the content provider 2, and the service provider 3 produces handling control information. Since processing in step S311 and processing in step S312 are the same as those in steps S291 and S292 of FIG. 52, repeated descriptions are omitted here. In step S313, the pricing section 42 of the service provider 3 decrypts the encrypted handling policy contained in the content-provider secure container. In step S314, on the basis of the handling policy, the pricing section 42 of the service provider 3 produces the handling control information which has been described in relation to FIG. 23. Since processing in step S315 through step S318 is the same as that in steps S294 through S297 of FIG. 52, repeated description is omitted.

[0174] As described above, the service provider 3 transmits to the receiver 51 a service-provider secure container containing the encrypted handling policy.

[0175] Next, with reference to the flowchart of FIG. 54, there will be described the processing which corresponds to step S16 of FIG. 34 and which enables the receiver 51 to perform charging processing after reception of a proper service-provider secure container. In step S331, the decryption/encryption module 74 of the receiver 51 judges whether the content key Kco can be decrypted by use of the distribution key Kd. When it is judged that the content key Kco cannot be decrypted by use of the distribution key Kd, in

step S332, the receiver 51 executes the processing for receiving the distribution key Kd, which has been described in relation to FIG. 48, and then proceeds to step S333. When it is judged in step S331 that the content key Kco can be decrypted by use of the distribution key Kd, the processing skips step S332 and proceeds to step S333. In step S333, the decryption unit 91 of the receiver 51 decrypts the content key Kco by use of the distribution key Kd, which has been stored in the storage module 73 through processing in step S13 of FIG. 34.

[0176] In step S334, the charging processing module 72 of the receiver 51 extracts the handling policy and the price information from the service-provider secure container and produces the charging information and the conditions-for-use information, which have been described with reference to FIGS. 19 and 20, respectively. In step S335, the charging processing module 72 of the receiver 51 judges whether the current charge is greater than the upper limit of charge, on the basis of the charging information stored in the storage module 73 and the charging information calculated in step S334. When the current charge is judged to be greater than the upper limit of charge, in step S336, the receiver 51 executes the processing for receiving the distribution key Kd, which has been described in relation to FIG. 48, to thereby obtain a new distribution key Kd. Subsequently, the receiver 51 proceeds to step S337. When it is judged in step S335 that the current charge is less than the upper limit of

charge, the receiver 51 skips steps 336 and proceeds to step S337.

[0177] In step S337, the charging processing module 72 of the receiver 51 stores the charging information in the storage module 73. In step S338, the charging processing module 72 of the receiver 51 stores in the HDD 52 the conditions-for-use information generated in step S334. In step S339, the SAM 62 of the receiver 51 registers in the HDD 52 the handling policy extracted from the service-provider secure container.

[0178] In step S340, the decryption/encryption module 74 of the receiver 51 applies the hash function to the conditions-for-use information to thereby calculate a hash value. In step S341, the storage module 73 of the receiver 51 stores the hash value of the conditions-for-use information. In the case in which the save key Ksave is not stored in the storage module 73, in step S342, the random-number generation unit 92 of the receiver 51 generates a random number serving as a save key Ksave. Subsequently, the receiver 51 proceeds to step S343. In the case in which the save key Ksave is stored in the storage module 73, the receiver 51 skips step S342 and proceeds to step S343.

[0179] In step S343, the encryption unit 93 of the receiver 51 encrypts the content key Kco by use of the save key Ksave. In step S344, the SAM 62 of the receiver 51 stores the encrypted content key Kco in the HDD 52. In the case in which the save key Ksave is not stored in the storage module

73, In step S345, the decryption/encryption module 74 of the receiver 51 stores the save key Ksave in the storage module 73. Subsequently, the receiver 51 ends the processing. In the case in which the save key Ksave is stored in the storage module 73, the receiver 51 skips step S345 and ends the processing.

[0180] In the above-described manner, the receiver 51 stores the charging information in the storage module 73, decrypts the content key Kco by use of the distribution key Kd, encrypts the content key Kco by use of the save key Ksave, and stores it in the HDD 52. The save key Ksave is stored in the storage module 73.

[0181] Through processing similar to the above-described processing, the recorder 53 stores the charging information in the storage module provided within the SAM 66, decrypts the content key Kco by use of the distribution key Kd, encrypts the content key Kco by use of the save key Ksave, and stores it in the HDD 52. The save key Ksave is stored in the storage module within the SAM 66.

[0182] With reference to the flowchart of FIG. 55, there will be described the processing which corresponds to step S17 of FIG. 34 and which enables the receiver 51 to reproduce content. In step S361, the decryption/encryption module 74 of the receiver 51 reads out of the HDD 52 the conditions-for-use information stored in step S338 of FIG. 54 and the encrypted content key Kco stored in step S344 of FIG. 54. In step S362, the decryption/encryption module 74 of the

receiver 51 applies the hash function to the conditions¹²-for-use information to calculate a hash value.

[0183] In step S363, the decryption/encryption module 74 of the receiver 51 judges whether the hash value calculated in step S362 coincides with hash value which was stored in the storage module 73 in step S340 of FIG. 54. When the hash value calculated in step S362 is judged to coincide with hash value stored in the storage module 73, in step S364, the decryption/encryption module 74 of the receiver 51 updates predetermined information, such as a value indicating the number of times of use, contained in the conditions-for-use information. In step S365, the decryption/encryption module 74 of the receiver 51 applies the hash function to the updated conditions-for-use information to thereby obtain a hash value. In step S366, the storage module 73 of the receiver 51 stores the hash value of the conditions-for-use information calculated in step S365. In step S367, the decryption/encryption module 74 of the receiver 51 records the updated conditions-for-use information in the HDD 52.

[0184] In step S368, the mutual authentication module 71 of the SAM 62 and the mutual authentication module 75 of the extension section 63 mutually authenticate, and the SAM 62 and the extension section 63 store the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. The random number R1, R2, or R3 used in the mutual authentication is used as a

temporary key Ktemp. In step S369, by use of the save key Ksave stored in the storage module 73, the decryption unit 91 of the decryption/encryption module 74 decrypts the content key Kco which was stored in the HDD 52 in step S344 of FIG. 54. In step S370, the encryption unit 93 of the decryption/encryption module 74 encrypts the decrypted content key Kco by use of the temporary key Ktemp. In step S371, the SAM 62 transmits to the extension section 63 the content key Kco having been encrypted by use of the temporary key Ktemp.

[0185] In step S372, the decryption module 76 of the extension section 63 decrypts the content key Kco by use of the temporary key Ktemp. In step S373, the SAM 62 reads the content recorded in the HDD 52 and transmits it to the extension section 63. In step S374, the decryption module 77 of the extension section 63 decrypts the content by use of the content key Kco. In step S375, the extension module 78 of the extension section 63 extends the decrypted content in accordance with a predetermined scheme such as ATRAC2. In step S376, the watermark addition module 79 of the extension section 63 inserts into the extended content a predetermined watermark that specifies the receiver 51. In step S377, the receiver 51 outputs the reproduced content to an unillustrated speaker or the like and then ends the processing.

[0186] When in step S363 the hash value calculated in step S362 is judged not to coincide with the hash value stored in

the storage module 73, in step S378, the SAM 62 performs predetermined error processing, such as processing for causing an unillustrated display unit to display an error message, and then ends the processing.

[0187] In the above-described manner, the receiver 51 reproduces the content.

[0188] FIG. 56 is a flowchart showing processing which the receiver 51 in the user home network 5 having the configuration shown in FIG. 11 performs in order to cause the decoder 56 to reproduce content. Since processing in steps S391 to S397 is the same as that in steps S361 to S367 of FIG. 55, repeated description is omitted here.

[0189] In step S398, the mutual authentication module 71 of the SAM 62 and the mutual authentication module 101 of the decoder 56 mutually authenticate and share the temporary key Ktemp. Since this authentication processing is similar to that having been described with reference to FIGS. 37 to 39, repeated description is omitted here. The random number R1, R2, or R3 used in the mutual authentication is used as a temporary key Ktemp. In step S399, by use of the save key Ksave stored in the storage module 73, the decryption unit 91 of the decryption/encryption module 74 decrypts the content key Kco which was stored in the HDD 52. In step S400, the encryption unit 93 of the decryption/encryption module 74 encrypts the decrypted content key Kco by use of the temporary key Ktemp. In step S401, the SAM 62 transmits to the decoder 56 the content key Kco having been encrypted by

use of the temporary key Ktemp.

[0190] In step S402, the decryption module 102 of the decoder 56 decrypts the content key Kco by use of the temporary key Ktemp. In step S403, the SAM 62 reads the content recorded in the HDD 52 and transmits it to the decoder 56. In step S404, the decryption module 103 of the decoder 56 decrypts the content by use of the content key Kco. In step S405, the extension module 104 of the decoder 56 extends the decrypted content in accordance with a predetermined scheme such as ATRAC2. In step S406, the watermark addition module 105 of the decoder 56 inserts into the extended content a predetermined watermark that specifies the decoder 56. In step S407, the decoder 56 outputs the reproduced content to an unillustrated speaker or the like and then ends the processing.

[0191] Since processing in step S408 is the same as that in step S378 of FIG. 55, repeated description is omitted here.

[0192] As described above, when the user home network 5 has the configuration shown in FIG. 11, the content received by the receiver 51 is reproduced at the decoder 56.

[0193] With reference to the flowchart of FIG. 57, there is described processing which enables the EMD service center 1 to produce a settlement object before performance of settlement processing, which will be described later with reference to FIG. 61. In step S421, the historical-data management section 15 of the EMD service center 1 selects charging information regarding use of specific content, among

a plurality pieces of charging information which the historical-data management section 15 has received from the user home network 5 and stores in, for example, step S187 or S189 of FIG. 47. Subsequently, the historical-data management section 15 transmits the selected charging information to the profit-distribution section 16. In step S422, the profit-distribution section 16 judges whether the charging information received from the historical-data management section 15 contains data showing profit distribution to the content provider 2 and the service provider 3. When the charging information received from the historical-data management section 15 is judged to contain data showing profit distribution to the content provider 2 and the service provider 3, the profit-distribution section 16 proceeds to step S423.

[0194] In step S423, with reference to the data contained in the charging information and indicating profit distribution, the profit-distribution section 16 calculates an amount of money which a user having utilized the specific content must pay to the service provider 3. In step S424, with reference to the data contained in the charging information and indicating profit distribution, the profit-distribution section 16 calculates an amount of money which the service provider 3 must pay to the content provider 2. In step S425, with reference to the data contained in the charging information and indicating profit distribution, the profit-distribution section 16 calculates an amount of money which

the content provider 2 must pay to the proprietary organization. Subsequently the profit-distribution section 16 proceeds to step S429.

[0195] When in step S422 the charging information received from the historical-data management section 15 is judged not to contain data showing profit distribution to the content provider 2 and the service provider 3, the profit-distribution section 16 proceeds to step S426. In step S426, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the user having utilized the specific content must pay to the service provider 3. In step S427, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the service provider 3 must pay to the content provider 2. In step S428, with reference to the profit-distribution database stored in the profit-distribution section 16, the profit-distribution section 16 calculates an amount of money which the content provider 2 must pay to the proprietary organization. Subsequently the profit-distribution section 16 proceeds to step S429.

[0196] In step S429, with reference to data of the discount information database stored in the profit-distribution section 16, the profit-distribution section 16 corrects the amount of money which the specific user must pay to the service provider 3, the amount of money which the service

provider 3 must pay to the content provider 2, and the amount of money which the content provider 2 must pay to the proprietary organization.

[0197] In step S430, the historical-data management section 15 judges whether the calculations in steps S423 to S429 have been performed for all the contents. When it is judged that the calculations in steps S423 to S429 have not yet been performed for all the contents, the historical-data management section 15 returns to step S421 in order to repeat the processing in step 421 and in subsequent steps. When it is judged in step S430 that the calculations in steps S423 to S429 have been performed for all the contents, the profit-distribution section 16 proceeds to step S431.

[0198] In step S431, for each user, the profit-distribution section 16 calculates an amount of money to be paid to each service provider 3 and produces a credit settlement object 1 (e.g., a credit settlement object 1 shown in FIG. 58(A) when the user pays the usage fee by use of a credit card). In the credit settlement object 1, the ID of the user is set as a payer; the ID of the service provider 3 is set as a receiver; and an amount of money to be paid to the service provider 3 is set as a payment amount. In step S432, for each service provider 3, the profit-distribution section 16 calculates an amount of money to be paid to each content provider 2 and produces a credit settlement object 2 (e.g., a credit settlement object 2 shown in FIG. 58(B) when the user pays the usage fee by use of a credit card). In the credit

settlement object 2, the credit settlement object 1 is set as a payer; the ID of the content provider 2 is set as a receiver; and an amount of money to be paid to the content provider 2 is set as a payment amount.

[0199] In step S433, for each content provider 2, the profit-distribution section 16 calculates an amount of money to be paid to the proprietary organization and produces a credit settlement object 3 (e.g., a credit settlement object 3 shown in FIG. 58(C) when the user pays the usage fee by use of a credit card). In the credit settlement object 3, the credit settlement object 1 is set as a payer; the ID of the proprietary organization is set as a receiver; and an amount of money to be paid to the proprietary organization is set as a payment amount. In step S434, with reference to the user's usage-fee table which is stored in the charge billing section 19 and which stores a usage fee that each user pays to the EMD service center 1, the charge billing section 19 calculates an amount of money to be collected from the user and produces a credit settlement object 4 (e.g., a credit settlement object 4 shown in FIG. 58(D) when the user pays the usage fee by use of a credit card). Further, the charge billing section 19 sets the collection money of the credit settlement object 1 and ends the processing. In the credit settlement object 4, the credit settlement object 1 is set as a payer; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 is set as a payment amount.

[0200] In the above-described manner, the EMD service center 1 produces a settlement object.

[0201] FIG. 59 is a diagram showing an example of a bank settlement object used when the service provider 3, the content provider 2, and the proprietary organization pay service charges to the EMD service center 1 by means of bank settlement. In a bank settlement object 1 shown in FIG. 59(A), the ID of the service provider 3 is set as a payer; an amount of money to be collected from the service provider 3 is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount. In a bank settlement object 2 shown in FIG. 59(B), the ID of the content provider 2 is set as a payer; an amount of money to be collected from the content provider 2 is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount. In a bank settlement object 3 shown in FIG. 59(C), the ID of the proprietary organization is set as a payer; an amount of money to be collected from the proprietary organization is set as a collection amount; the ID of the EMD service center 1 is set as a receiver; and an amount of money to be paid to the EMD service center 1 (equal to the collection amount) is set as a payment amount.

[0202] FIG. 60 is a diagram showing an example of a

settlement object used when each user pays fees by use of a credit card; and the service provider 3 and the content provider 2 perform settlement by use of their bank accounts. Since the credits settlement objects of FIGS. 60(A) and 60(D) are the same as those of FIGS. 58(A) and 58(D), repeated descriptions are omitted. In a bank settlement object 2 shown in FIG. 60(B), the ID of the service provider 3 is set as a payer; an amount of money to be collected from the service provider 3 (the sum of an amount of money to be paid to the content provider 2 and an amount of money to be paid to the proprietary organization) is set as a collection amount; the ID of the content provider 2 is set as a receiver; and an amount of money to be paid to the content provider 2 (equal to the collection amount) is set as a payment amount. In a bank settlement object 3 shown in FIG. 60(C), the ID of the content provider 2 is set as a payer; an amount of money to be collected from the content provider 2 is set as a collection amount; the ID of the proprietary organization is set as a receiver; and an amount of money to be paid to the proprietary organization (equal to the collection amount) is set as a payment amount.

[0203] Upon execution of settlement on the basis of the payers, collection amounts, receivers, and payment amounts described in the settlement objects of FIGS. 58, 59, and 60, predetermined amounts of money are paid to the EMD service center 1, the content provider 2, the service provider 3, and the proprietary organization. Processing which enables the

EMD service center 1 to perform settlement while using a credit settlement object will be described with reference to the flowchart of FIG. 61. In step S451, the treasury section 20 of the EMD service center 1 obtains a settlement institute, such as a bank, which serves as a receiver, from an ID which is described as a receiver in the credit settlement object. In step S452, the treasury section 20 of the EMD service center 1 obtains a settlement institute, such as a credit company, which serves as a payer, from an ID which is described as a payer in the credit settlement object. In step S453, on the basis of previously stored information, the treasury section 20 judges whether credit-check processing must be performed for the payer. When it is judged that credit-check processing for the payer is necessary, in step S454, the treasury section 20 performs the credit-check processing. When the credit-check processing performed in step S454 has revealed that the payer cannot make payment, the treasury section 20 ends the processing. When the credit-check processing performed in step S454 has revealed that the payer can make payment, the treasury section 20 proceeds to step S455.

[0204] When it is judged in step S453 that credit-check processing for the payer is unnecessary, the treasury section 20 skips step S454 and proceeds to step S455.

[0205] In step S455, the treasury section 20 judges whether the processing for the previous settlement object has been completed. When it is judged that the processing for the

previous settlement object has been completed, the treasury section 20 proceeds to step S456 and transmits to the settlement institutes obtained in steps S451 and S452 respective settlement instructions which correspond to the collection amount and payment amount described in the credit settlement object. In step S457, the treasury section 20 transmits the information regarding the settlement processing performed in step S456 to a receiver corresponding to the ID which is described as a receiver in the credit settlement object. In step S458, the treasury section 20 transmits the information regarding the settlement processing performed in step S456 to a payer corresponding to the ID which is described as a payer in the credit settlement object. Subsequently, the treasury section 20 ends the processing.

[0206] When it is judged in step S455 that the processing for the previous settlement object has not been completed, the treasury section 20 proceeds to step S459 and executes predetermined error processing for incomplete settlement; such as processing for transmitting a predetermined message to a payer which is described in the settlement object, processing for which has not been completed.

[0207] In the above-described manner, settlement using credit settlement objects is performed.

[0208] FIG. 62 is a flowchart showing processing which enables the EMD service center 1 to perform settlement while using bank settlement objects. This processing is equivalent to processing which is obtained by removing processing for

credit check (steps S451 and S454) from the settlement processing using credit settlement objects shown in FIG. 61. Since processing in steps S471 and S472 is the same as that in steps S451 and S452 of FIG. 61, repeated description is omitted here. Since processing in steps S473 to S477 is the same as that in steps S455 to S459 of FIG. 61, repeated description is omitted here.

[0209] In the above-described manner, settlement using bank settlement objects is processed together with settlement using credit settlement objects. Thus, predetermined amounts of money are collected from users, the content provider 2, the service provider 3, and the proprietary organization; and predetermined amounts of money are transferred to the EMD service center 1, the content provider 2, the service provider 3, and the proprietary organization.

[0210] The embodiment has been described while music data were used as example content. However, contents are not limited to music data and may be dynamic image data, static image data, document data, or program data. When these data are distributed, a compression scheme suitable for the type of content (e.g., MPEG (Moving Picture Experts Group) for image data) is used. As to watermarks, a watermark suitable for the type of content is used.

[0211] The common key cryptosystem has been described while DES, which is a block cryptosystem, was used as an example. However, FEAL proposed by NTT (Trademark), IDEA (International Data Encryption Algorithm), or stream

cryptosystem in which encryption is performed for each unit consisting of one bit to a few bits may be used.

[0212] In the embodiment, content and a content key K_{co} are encrypted in common key cryptosystem. However, a public key cryptosystem may be used.

[0213] In the present specification, the term "system" refers to the entire apparatus consisting of a plurality of apparatuses.

[0214] Examples of a provision medium for providing users with a computer program for performing the above-described processing include recording media such as a magnetic disk, a CD-ROM, and solid memories, as well as communication media such as a network and a satellite.

[0215]

[Effect of the Invention] In the information processing apparatus described in claim 1, the information processing method described in claim 6, and the provision medium described in claim 7, data which specify the information, and data which indicate an amount to be paid to each of the information providers for use of the information are stored; the sum total of amounts to be paid to each of the information providers is calculated on the basis of the stored data; and an instruction is issued to a settlement institute to perform settlement for each of the information providers, on the basis of profits gained by each of the information providers. Therefore, settlement processing and profit-calculation processing can be performed more

efficiently.

[Brief Description of the Drawings]

[FIG. 1] Diagram for explaining an EMD system.

[FIG. 2] Block diagram showing the functional configuration of the EMD service center 1.

[FIG. 3] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 4] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 5] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 6] Diagram for explaining transmission of distribution keys Kd by the EMD service center 1.

[FIG. 7] Diagram for explaining the user-registration data base.

[FIG. 8] Block diagram showing the functional configuration of the content provider 2.

[FIG. 9] Block diagram showing the functional configuration of the service provider 3.

[FIG. 10] Block diagram showing the configuration of the user home network 5.

[FIG. 11] Block diagram showing the configuration of the user home network 5.

[FIG. 12] Diagram for describing a content and information accompanying the content.

[FIG. 13] Diagram for explaining a content-provider secure container.

[FIG. 14] Diagram for explaining a certificate of the content provider 2.

[FIG. 15] Diagram for explaining a service-provider secure container.

[FIG. 16] Diagram for explaining a certificate of the service provider 3.

[FIG. 17] Diagram showing a handling policy, price information, and conditions-for-use information.

[FIG. 18] Diagram for explaining single copying and multiple copying.

[FIG. 19] Diagram for explaining a handling policy and price information.

[FIG. 20] Diagram for explaining a handling policy, price information, and conditions-for-use information.

[FIG. 21] Diagram for explaining another configuration of a content and information accompanying the content.

[FIG. 22] Diagram for explaining a service-provider secure container.

[FIG. 23] Diagram showing a configuration of a handling policy, handling control information, price information, and conditions-for-use information.

[FIG. 24] Diagram for explaining another configuration of a content and information accompanying the content.

[FIG. 25] Diagram for explaining a content-provider secure container.

[FIG. 26] Diagram for explaining a service-provider secure container.

[FIG. 27] Diagram for explaining the operation of the EMD service center 1 for collecting data necessary for settlement processing.

[FIG. 28] Diagram showing an example of the profit-distribution data base.

[FIG. 29] Diagram showing an example of the discount table.

[FIG. 30] Diagram showing an example of the user's usage-fee table.

[FIG. 31] Diagram for explaining the operation of the EMD service center 1 when receiving charging information from the user home network 5.

[FIG. 32] Diagram for explaining the operation of the EMD service center 1 for profit distribution processing.

[FIG. 33] Diagram for explaining the operation of the EMD service center 1 for transmitting to the JASRAC information regarding past use of contents.

[FIG. 34] Flowchart for explaining processing for content distribution.

[FIG. 35] Flowchart for explaining processing for content distribution.

[FIG. 36] Flowchart for explaining processing which enables the EMD service center 1 to transmits distribution keys Kd to the content provider 2.

[FIG. 37] Flowchart for explaining the operation of mutual authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 38] Flowchart for explaining the operation of mutual

authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 39] Flowchart for explaining the operation of mutual authentication performed between the content provider 2 and the EMD service center 1.

[FIG. 40] Flowchart for explaining processing which enables registration of the receiver 51 in the EMD service center 1.

[FIG. 41] Diagram for explaining a certificate of the SAM.

[FIG. 42] Diagram for explaining a registration list.

[FIG. 43] Flowchart for explaining processing for transferring data of the SAM 62 to the IC card 55 for backup.

[FIG. 44] Flowchart for explaining processing for transferring data of the SAM 62 to the IC card 55 for backup.

[FIG. 45] Flowchart for explaining processing for causing a new receiver to read backup data from the IC card 55.

[FIG. 46] Flowchart for explaining processing for causing a new receiver to read backup data from the IC card 55.

[FIG. 47] Flowchart for explaining processing which enables the receiver 51 to register the recorder 53 depending thereon in the EMD service center 1.

[FIG. 48] Flowchart for explaining processing which enables the receiver 51 to receive the distribution key Kd from the EMD service center 1.

[FIG. 49] Flowchart for explaining processing which enables the recorder to receive the distribution key Kd.

[FIG. 50] Flowchart for explaining processing which enables the content provider 2 to transmit a content-provider secure

container to the service provider 3.

[FIG. 51] Flowchart for explaining another processing which enables the content provider 2 to transmit a content-provider secure container to the service provider 3.

[FIG. 52] Flowchart for explaining processing which enables the service provider 3 to transmit a service-provider secure container to the receiver 51.

[FIG. 53] Flowchart for explaining processing which enables the service provider 3 to transmit a service-provider secure container to the receiver 51.

[FIG. 54] Flowchart for explaining charging processing of the receiver 51.

[FIG. 55] Flowchart for explaining processing which enables the receiver 51 to reproduce content.

[FIG. 56] Flowchart for explaining processing which enables the receiver 51 to cause the decoder 56 to reproduce the content.

[FIG. 57] Flowchart for explaining settlement-object-production processing of the EMD service center 1.

[FIG. 58] Diagram showing an example of a credit settlement object.

[FIG. 59] Diagram showing an example of a bank settlement object.

[FIG. 60] Diagram showing an example of the credit settlement object and the bank settlement object..

[FIG. 61] Flowchart for explaining credit settlement processing.

[FIG. 62] Flowchart for explaining bank settlement processing.

[Description of Reference Numerals]

1: EMD service center, 2: content provider, 3: service provider, 5: user home network, 15: historical-data management section, 16: profit-distribution section, 18: user management section, 20: treasury section, 42: pricing section, 51: receiver, 56: decoder, 61: communication section, 62: SAM, 63: extension section, 71: mutual authentication module, 72: charge module, 73: storage module, 74: decryption/encryption module, 75: mutual authentication module, 76: decryption module, 77: decryption module, 81: mutual authentication module, 91: decryption unit, 92: encryption unit, 93: encryption unit, 101: mutual authentication module, 102: decryption module, 103: decryption module

FIG. 1

- 1: EMD SERVICE CENTER
- 2: CONTENT PROVIDER
- 3: SERVICE PROVIDER
- 4: NETWORK
- 5: USER HOME NETWORK

FIG. 2

- 11: SERVICE-PROVIDER MANAGEMENT SECTION
- 12: CONTENT-PROVIDER MANAGEMENT SECTION
- 13: COPY-RIGHT MANAGEMENT SECTION
- 14: KEY SERVER
- 15: HISTORICAL-DATA MANAGEMENT SECTION
- 16: PROFIT-DISTRIBUTION SECTION
- 17: MUTUAL AUTHENTICATION SECTION
- 18: USER MANAGEMENT SECTION
- 19: CHARGE BILLING SECTION
- 20: TREASURY SECTION
- 21: AUDITOR SECTION
- A: EMD SERVICE CENTER 1

FIG. 3

- A: DISTRIBUTION KEY HELD BY CONTENT PROVIDER
- B: DISTRIBUTION KEY HELD BY EMD SERVICE CENTER
- C: DISTRIBUTION KEY HELD BY RECEIVER
- D: DISTRIBUTION KEYS TO BE USED
- E: DISTRIBUTION KEY

F: VERSION OF DISTRIBUTION KEY
G: USABLE PERIOD
H: START
I: END
J: TRANSMISSION OF DISTRIBUTION KEYS

FIG. 4

SAME AS FIG. 3

FIG. 5

SAME AS FIG. 3

FIG. 6

SAME AS FIG. 3

FIG. 7

A: ID
B: SETTLEMENT PROCESSING
C: REGISTRATION
D: CONNECTION WITH EMD SERVICE CENTER
E: POSSIBLE
F: IMPOSSIBLE

FIG. 8

31: CONTENT SERVER
32: WATERMARK ADDING SECTION
33: COMPRESSION SECTION

34: ENCRYPTION SECTION
35: RANDOM-NUMBER GENERATION SECTION
36: ENCRYPTION SECTION
37: POLICY STORAGE SECTION
38: SECURE CONTAINER CREATION SECTION
39: MUTUAL AUTHENTICATION SECTION
A: CONTENT PROVIDER 2

FIG 9

41: CONTENT SERVER
42: PRICING SECTION
43: POLICY STORAGE SECTION
44: SECURE CONTAINER CREATION SECTION
45: MUTUAL AUTHENTICATION SECTION
A: SERVICE PROVIDER 3

FIG. 10

51: RECEIVER
52: HDD
53: RECORDER
54: MD DRIVE
55: IC CARD
61: COMMUNICATION SECTION
62: SAM
63: EXTENSION SECTION
64: IC CARD INTERFACE
65: RECORD/REPRODUCTION SECTION

66: SAM
67: EXTENSION SECTION
71: MUTUAL AUTHENTICATION MODULE
72: CHARGE MODULE
73: STORAGE MODULE
74: DECRYPTION/ENCRYPTION MODULE
75: MUTUAL AUTHENTICATION MODULE
76: DECRYPTION MODULE
77: DECRYPTION MODULE
78: EXTENSION MODULE
79: WATERMARK ADDITION MODULE
80: MUTUAL AUTHENTICATION MODULE
81: STORAGE MODULE
91: DECRYPTION UNIT
92: RANDOM-NUMBER GENERATION UNIT
93: ENCRYPTION UNIT
A: USER HOME NETWORK 5

FIG. 11

56: DECODER
101: MUTUAL AUTHENTICATION MODULE
102: DECRYPTION MODULE
103: DECRYPTION MODULE
104: EXTENSION MODULE
105: WATERMARK ADDITION MODULE
A: USER HOME NETWORK 5

OTHER ELEMENTS ARE THE SAME AS THOSE SHOWN IN FIG. 10

FIG. 12

- 1: EMD SERVICE CENTER
- 2: CONTENT PROVIDER
- 3: SERVICE PROVIDER
- 5: USER HOME NETWORK
- A: CONTENT
- B: CONTENT KEY
- C: HANDLING POLICY
- D: PRICE INFORMATION
- E: CONDITIONS-FOR-USE INFORMATION
- F: CHARGING INFORMATION
- G: ENCRYPTED INFORMATION
- H: INFORMATION WITH SIGNATURE

FIG. 13

- A: CONTENT-PROVIDER SECURE CONTAINER
- B: CONTENT KEY K_{co}
- C: CONTENT
- D: DISTRIBUTION KEY K_d
- E: HANDLING POLICY
- F: PRIVATE KEY K_{scp} OF CONTENT PROVIDER
- G: SIGNATURE
- H: HASH FUNCTION

FIG. 14

- A: CERTIFICATE OF CONTENT PROVIDER

B: VERSION NUMBER OF CERTIFICATE
C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION
OFFICE HAS ALLOCATED
D: ALGORITHM AND PARAMETERS USED IN SIGNATURE
E: NAME OF AUTHENTICATION OFFICE
F: VALID TERM OF CERTIFICATE
G: NAME (ID) OF CONTENT PROVIDER
H: PUBLIC KEY K_{pcp} OF CONTENT PROVIDER
I: PRIVATE KEY K_{sca} OF AUTHENTICATION OFFICE
J: SIGNATURE
K: HASH FUNCTION

FIG 15

A: SERVICE PROVIDER SECURE CONTAINER
B: CONTENT KEY K_{co}
C: CONTENT
D: DISTRIBUTION KEY K_d
E: HANDLING POLICY
F: PRICE INFORMATION
G: PRIVATE KEY K_{ssp} OF SERVICE PROVIDER
H: SIGNATURE
I: HASH FUNCTION

FIG. 16

A: CERTIFICATE OF SERVICE PROVIDER
B: VERSION NUMBER OF CERTIFICATE
C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION

OFFICE HAS ALLOCATED

D: ALGORITHM AND PARAMETERS USED IN SIGNATURE

E: NAME OF AUTHENTICATION OFFICE

F: VALID TERM OF CERTIFICATE

G: NAME (ID) OF SERVICE PROVIDER

H: PUBLIC KEY K_{psp} OF SERVICE PROVIDER

I: PRIVATE KEY K_{sca} OF AUTHENTICATION OFFICE

J: SIGNATURE

K: HASH FUNCTION

FIG. 17

A: HANDLING POLICY

B: ITEMS OF USE

C: REPRODUCTION

D: SINGLE COPYING

E: MULTICOPYING

F: POSSIBLE/IMPOSSIBLE

G: HANDLING POLICY AND PRICE INFORMATION

H: PRICE

I: 150 YEN

J: 80 YEN

K: CONDITIONS-FOR-USE INFORMATION

FIG. 18

A: MULTICOPYING

B: SINGLE COPYING

C: ORIGINAL

D: COPY

FIG. 19

A: ITEMS OF USE

B: REPRODUCTION

C: SINGLE COPY

D: MULTIPLE COPY

E: HANDLING POLICY AND PROFIT DISTRIBUTION

F: POSSIBLE/IMPOSSIBLE

G: PROFIT DISTRIBUTION

H: HANDLING POLICY, PROFIT DISTRIBUTION, AND PRICE
INFORMATION

I: DISTRIBUTION PRICE

J: CHARGING INFORMATION

K: NUMBER OF TIMES OF USE

L: 70 YEN

M: 40 YEN

N: 60 YEN

O: 150 YEN

P: 30 YEN

Q: 80 YEN

FIG. 20

A: HANDLING POLICY AND PRICE INFORMATION

B: ITEMS OF USE

C: REPRODUCTION

D: LIMITLESS

E: LIMITED NUMBER OF TIMES
F: LIMITED PERIOD
G: PRICE
H: 60 YEN
I: 90 YEN
J: CONDITIONS-FOR-USE INFORMATION

FIG. 21

1: EMD SERVICE CENTER
2: CONTENT PROVIDER
3: SERVICE PROVIDER
5: USER HOME NETWORK
A: CONTENT
B: CONTENT KEY
C: HANDLING POLICY
D: PRICE INFORMATION
E: CONDITIONS-FOR-USE INFORMATION
F: CHARGING INFORMATION
H: ENCRYPTED INFORMATION
I: INFORMATION WITH SIGNATURE
G: HANDLING CONTROL INFORMATION

FIG. 22

A: CONTENT-PROVIDER SECURE CONTAINER
B: CONTENT KEY K_{co}
C: CONTENT
D: DISTRIBUTION KEY K_d

E: HANDLING POLICY
F: HANDLING CONTROL INFORMATION
G: PRICE INFORMATION
H: PRIVATE KEY Kssp OF SERVICE PROVIDER
I: SIGNATURE
J: HASH FUNCTION

FIG. 23

A: ITEMS OF USE
B: REPRODUCTION
C: SINGLE COPYING
D: MULTICOPYING
E: POSSIBLE/IMPOSSIBLE
F: PRICE
G: CONDITIONS-FOR-USE INFORMATION
H: 150 YEN
I: 80 YEN
J: HANDLING POLICY
K: HANDLING CONTROL INFORMATION AND PRICE INFORMATION

FIG. 24

1: EMD SERVICE CENTER
2: CONTENT PROVIDER
3: SERVICE PROVIDER
5: USER HOME NETWORK
A: CONTENT
B: CONTENT KEY

C: HANDLING POLICY
D: PRICE INFORMATION
E: CONDITIONS-FOR-USE INFORMATION
F: CHARGING INFORMATION
G: HANDLING CONTROL INFORMATION
H: ENCRYPTED INFORMATION

FIG. 25

A: CONTENT-PROVIDER SECURE CONTAINER
B: CONTENT KEY K_{co}
C: CONTENT
D: DISTRIBUTION KEY K_d
E: HANDLING POLICY
F: PRIVATE KEY K_{scp} OF CONTENT PROVIDER
G: SIGNATURE
H: HASH FUNCTION

FIG. 26

A: SERVICE-PROVIDER SECURE CONTAINER
B: CONTENT KEY K_{co}
C: CONTENT
D: DISTRIBUTION KEY K_d
E: HANDLING POLICY
F: HANDLING CONTROL INFORMATION
G: PRICE INFORMATION
H: PRIVATE KEY K_{ssp} OF SERVICE PROVIDER

I: SIGNATURE

J: HASH FUNCTION

FIG. 27

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

A: CONTENT-PROVIDER REGISTRATION DATA

B:: CONTENT-PROVIDER ID

C: SERVICE-PROVIDER REGISTRATION DATA

D: SERVICE-PROVIDER ID

E: USER ID

F: USER-REGISTRATION DATA

FIG. 28

A: CONTENT ID

B: CONTENT-PROVIDER ID

C: PROPRIETOR ORGANIZATION

FIG. 29

A: PROVIDER ID

B: CONTENT PROVIDER 1

C: CONTENT PROVIDER 2

D: SERVICE PROVIDER 1

E: SERVICE PROVIDER 2

F: CONTENT ID

G: DISCOUNT RATE

H: PERIOD

I: ALL CONTENTS

FIG. 30

A: MONTHLY BASIC CHARGE

B: 1000 YEN

C: PERIOD

D: USAGE FEE

E: ADJUSTMENT AMOUNT

F: ABOVE 3000 YEN

FIG. 31

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

3: SERVICE PROVIDER

5: USER HOME NETWORK

11: SERVICE-PROVIDER MANAGEMENT SECTION

12: CONTENT-PROVIDER MANAGEMENT SECTION

13: COPY-RIGHT MANAGEMENT SECTION

14: KEY SERVER

15: HISTORICAL-DATA MANAGEMENT SECTION

16: PROFIT-DISTRIBUTION SECTION

17: MUTUAL AUTHENTICATION SECTION

18: USER MANAGEMENT SECTION

19: CHARGE BILLING SECTION

20: TREASURY SECTION

21: AUDITOR SECTION

FIG. 32

SAME AS FIG. 31

FIG. 33

SAME AS FIG. 31

FIG. 34

A: START CONTENT DISTRIBUTION PROCESSING

S11: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO
CONTENT PROVIDER, AND CONTENT PROVIDER RECEIVES DISTRIBUTION
KEYS

S12: USER REGISTERS APPARATUS INFORMATION IN EMD SERVICE
CENTER

S13: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO USER,
AND USER RECEIVES DISTRIBUTION KEYS

S14: CONTENT PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE
PROVIDER, AND SERVICE PROVIDER RECEIVES SECURE CONTAINER

S15: SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER, AND
USER RECEIVES SECURE CONTAINER

S16: USER PERFORMS CHARGING PROCESSING

S17: USER REPRODUCES CONTENT

B: END

FIG. 35

A: START CONTENT DISTRIBUTION PROCESSING

S21: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO
CONTENT PROVIDER, AND CONTENT PROVIDER RECEIVES DISTRIBUTION
KEYS

S22: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO
SERVICE PROVIDER, AND SERVICE PROVIDER RECEIVES DISTRIBUTION
KEYS

S23: USER REGISTERS APPARATUS INFORMATION IN EMD SERVICE
CENTER

S24: EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEYS TO USER,
AND USER RECEIVES DISTRIBUTION KEYS

S25: CONTENT PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE
PROVIDER, AND SERVICE PROVIDER RECEIVES SECURE CONTAINER

S26: SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER, AND
USER RECEIVES SECURE CONTAINER

S27: USER PERFORMS CHARGING PROCESSING

S28: USER REPRODUCES CONTENT

B: END

FIG. 36

A: START PROCESSING FOR TRANSMITTING DISTRIBUTION KEYS TO
CONTENT PROVIDER

S31: MUTUAL AUTHENTICATION WITH CONTENT PROVIDER

S32: CONTENT PROVIDER RECEIVES DISTRIBUTION KEYS

S33: CONTENT PROVIDER STORES DISTRIBUTION KEYS

B: RETURN

FIG. 37

1: EMD SERVICE CENTER
2: CONTENT PROVIDER
S41: GENERATE RANDOM NUMBER R1 OF 64 BITS
S42: ENCRYPT R1 BY USE OF KEY Kc
S43: TRANSMIT ENCRYPTED R1 TO EMD SERVICE CENTER
S44: DECRYPT RECEIVED R1
S45: GENERATE RANDOM NUMBER R2 OF 32 BITS
S46: REPLACE LOWER 32 BITS OF RANDOM NUMBER R1 WITH RANDOM
NUMBER R2 TO THEREBY OBTAIN $R1_H || R2$
S47: ENCRYPT $R1_H || R2$ BY USE OF KEY Kc
S48: TRANSMIT ENCRYPTED $R1_H || R2$ TO CONTENT PROVIDER
S49: DECRYPT RECEIVED $R1_H || R2$
S50: AUTHENTICATE EMD SERVICE CENTER WHEN UPPER 32 BITS
OF DECRYPTED $R1_H || R2$ COINCIDE
S51: GENERATE RANDOM NUMBER R3 OF 32 BITS
S52: FORM $R2 || R3$
S53: ENCRYPT $R2 || R3$ BY USE OF KEY Kc
S54: TRANSMIT ENCRYPTED $R2 || R3$ TO EMD SERVICE CENTER
S55: DECRYPT RECEIVED $R2 || R3$
S56: AUTHENTICATE CONTENT PROVIDER WHEN UPPER 32 BITS
OF $R2 || R3$ COINCIDE

FIG. 38

1: EMD SERVICE CENTER
2: CONTENT PROVIDER
S61: GENERATE RANDOM NUMBER R1 OF 64 BITS
S62: ENCRYPT R1 BY USE OF KEY Kc1

S63: TRANSMIT ENCRYPTED R1 TO EMD SERVICE CENTER
 S64: DECRYPT RECEIVED R1
 S65: ENCRYPT R1 BY USE OF KEY Kc2
 S66: GENERATE RANDOM NUMBER R2 OF 64 BITS
 S67: ENCRYPT R2 BY USE OF KEY Kc2
 S68: TRANSMIT ENCRYPTED R1 AND R2 TO CONTENT PROVIDER
 S69: DECRYPT RECEIVED R1 AND R2
 S70: AUTHENTICATE EMD SERVICE CENTER WHEN DECRYPTED R1
 COINCIDE
 S71: ENCRYPT R2 BY USE OF KEY Kc1
 S72: TRANSMIT ENCRYPTED R2 TO EMD SERVICE CENTER
 S73: DECRYPT RECEIVED R2
 S74: AUTHENTICATE CONTENT PROVIDER WHEN DECRYPTED R2 COINCIDE

FIG. 39

1: EMD SERVICE CENTER

2: CONTENT PROVIDER

S81: GENERATE RANDOM NUMBER R1 OF 64 BITS
 S82: TRANSMIT R1 AND CERTIFICATE TO EMD SERVICE CENTER
 S83: CHECK SIGNATURE OF CERTIFICATE AND WHEN PROPER, EXTRACT
 PUBLIC KEY Kpcp FROM CERTIFICATE
 S84: GENERATE RANDOM NUMBER R2 OF 64 BITS
 S85: FORM $R1 || R2$
 S86: ENCRYPT $R1 || R2$ BY USE OF PRIVATE KEY Ksesc
 S87: ENCRYPT $R1 || R2$ BY USE OF PUBLIC KEY Kpcp
 S88: TRANSMIT TO CONTENT PROVIDER $R1 || R2$ ENCRYPTED BY USE OF
 PRIVATE KEY Ksesc, $R1 || R2$ ENCRYPTED BY USE OF PUBLIC KEY Kpcp,

AND CERTIFICATE

S89: CHECK SIGNATURE OF CERTIFICATE AND WHEN PROPER, EXTRACT
PUBLIC KEY K_{pesc} FROM CERTIFICATE

S90: DECRYPT $R1 || R2$ BY USE OF PUBLIC KEY K_{pesc}

S91: DECRYPT $R1 || R2$ BY USE OF PRIVATE KEY K_{scp}

S92: AUTHENTICATE EMD SERVICE CENTER WHEN DECRYPTED $R1 || R2$
COINCIDE

S93: GENERATE RANDOM NUMBER $R3$ OF 64 BITS

S94: FORM $R2 || R3$

S95: ENCRYPT $R2 || R3$ BY USE OF PUBLIC KEY K_{pesc}

S96: TRANSMIT ENCRYPTED $R2 || R3$ TO EMD SERVICE CENTER

S97: DECRYPT $R2 || R3$ BY USE OF PRIVATE KEY K_{sesc}

S98: AUTHENTICATE CONTENT PROVIDER WHEN DECRYPTED $R2$ COINCIDE

FIG. 40

A: START REGISTRATION PROCESSING

S101: IS IC CARD FOR BACKUP ATTACHED?

S102: PROCESSING FOR READING BACKUP

S103: SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER AND
TRANSMITS CERTIFICATE

S104: SAM ENCRYPTS INFORMATION OF SETTLEMENT INSTITUTE OF
USER, ETC. BY USE OF TEMPORARY KEY AND TRANSMITS THEM TO EMD
SERVICE CENTER

S105: EMD SERVICE CENTER SEARCHES REGISTRATION DATA BASE BY
USE OF ID OF SAM

S106: IS SAM OF RECEIVED ID REGISTERABLE?

S107: IS SAM OF RECEIVED ID NEW REGISTRATION?

S108: EMD SERVICE CENTER PRODUCES REGISTRATION LIST OF UPDATE
REGISTRATION

S109: EMD SERVICE CENTER TRANSFERS TO SAM DISTRIBUTION KEY
ENCRYPTED BY USE OF TEMPORARY KEY

S110: SAME DECRYPTS AND STORES RECEIVED DISTRIBUTION KEY

S111: EMD SERVICE CENTER TRANSMITS TO SAM REGISTRATION LIST
ENCRYPTED BY USE OF TEMPORARY KEY

S112: SAM DECRYPTS AND STORES RECEIVED REGISTRATION LIST

S113: EMD SERVICE CENTER PRODUCES REGISTRATION LIST OF
REGISTRATION DENIAL

S114: EMD SERVICE CENTER PRODUCES NEW REGISTRATION LIST

B: RETURN

FIG. 41

A: CERTIFICATE OF SAM

B: VERSION NUMBER OF CERTIFICATE

C: SERIAL NUMBER OF CERTIFICATE WHICH AUTHENTICATION
OFFICE HAS ALLOCATED

D: ALGORITHM AND PARAMETERS USED IN SIGNATURE

E: NAME OF AUTHENTICATION OFFICE

F: VALID TERM OF CERTIFICATE

G: NAME (ID) OF SAM

H: PUBLIC KEY K_{pu} OF SAM

I: PARAMETER INDICATING WHERE TO DEPEND ON ANOTHER SAM

J: PRIVATE KEY K_{sca} OF AUTHENTICATION OFFICE

K: SIGNATURE

L: HASH FUNCTION

FIG. 42

A: ID OF SAM
B: REGISTRATION DENIAL FLAG
C: STATUS FLAG
D: CONDITION FLAG
E: SIGNATURE

FIG. 43

A: START BACKUP OF STORAGE DATA OF SAM
S121: SAM MUTUALLY AUTHENTICATES WITH IC CARD
S122: GENERATE RANDOM NUMBER AS BACKUP KEY
S123: ENCRYPT STORAGE DATA OF SAM BY USE OF BACKUP KEY
S124: ENCRYPT BACKUP KEY BY USE OF PUBLIC KEY OF EMD SERVICE
CENTER
S125: STORE ENCRYPTED STORAGE DATA OF SAM AND ENCRYPTED
BACKUP KEY IN IC CARD
B: END

FIG. 44

A: START BACKUP OF STORAGE DATA OF SAM
S131: SAM MUTUALLY AUTHENTICATES WITH IC CARD
S132: ENCRYPT STORAGE DATA OF SAM BY USE OF PUBLIC KEY OF EMD
SERVICE CENTER
S133: STORE ENCRYPTED STORAGE DATA OF SAM IN IC CARD
B: END

FIG. 45

A: START PROCESSING FOR READING BACKUP INTO NEW RECEIVER

S141: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S142: READ ENCRYPTED STORAGE DATA OF SAM AND ENCRYPTED BACKUP
KEY FROM IC CARD

S143 SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S144: SAM TRANSMITS ENCRYPTED STORAGE DATA OF SAM AND
ENCRYPTED BACKUP KEY TO EMD SERVICE CENTER

S145: EMD SERVICE CENTER DECRYPTS BACKUP KEY BY USE OF
PRIVATE KEY

S146: EMD SERVICE CENTER DECRYPTS STORAGE DATA OF SAM BY USE
OF BACKUP KEY

S147: EMD SERVICE CENTER ENCRYPTS STORAGE DATA OF SAM BY USE
OF TEMPORARY KEY

S148: EMD SERVICE CENTER TRANSMITS STORAGE DATA OF SAM

S149: SAM DECRYPTS AND STORES RECEIVED DATA

S150: EMD SERVICE CENTER MAKES ID OF OLD SAM UN-REGISTERABLE
RETURN

FIG. 46

A: START PROCESSING FOR READING BACKUP INTO NEW RECEIVER

S161: SAM MUTUALLY AUTHENTICATES WITH IC CARD

S162: READ ENCRYPTED STORAGE DATA OF SAM FROM IC CARD

S163 SAM MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S164: SAM TRANSMITS ENCRYPTED STORAGE DATA OF SAM TO EMD
SERVICE CENTER

S165: EMD SERVICE CENTER DECRYPTS STORAGE DATA OF SAM BY USE

OF PRIVATE KEY

S166: EMD SERVICE CENTER ENCRYPTS STORAGE DATA OF SAM BY USE
OF TEMPORARY KEY

S167: EMD SERVICE CENTER TRANSMITS STORAGE DATA OF SAM

S168: SAM DECRYPTS AND STORES RECEIVED DATA

S169: EMD SERVICE CENTER MAKES ID OF OLD SAM UN-REGISTERABLE
RETURN

FIG. 47

A: START PROCESSING FOR REGISTERING RECORDER

S181: RECEIVER ADDS ID OF RECORDER INTO REGISTRATION LIST

S182: RECEIVER AND EMD SERVICE CENTER PERFORM MUTUAL
AUTHENTICATION

S183: IS RECEIVER UN-REGISTERABLE?

S184: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF
DISTRIBUTION KEY OF RECEIVER, CHARGING INFORMATION, HANDLING
POLICY, AND REGISTRATION LIST, WHICH HAVE BEEN ENCRYPTED BY
USE OF TEMPORARY KEY

S185: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, PROCESSES
CHARGING INFORMATION, AND UPDATES REGISTRATION LIST

S186: IS DISTRIBUTION KEY OF RECEIVER NEWEST VERSION?

S187: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND
CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF
TEMPORARY KEY, AND RECEIVER RECEIVES AND STORES REGISTRATION
LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S188: RECEIVER ERASES CHARGING INFORMATION AND UPDATES
REGISTRATION LIST

S189: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST,
CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY
ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND
STORES REGISTRATION LIST, CHARGING-INFORMATION RECEIPT
MESSAGE, AND DISTRIBUTION KEY

S190: RECEIVER ERASES CHARGING INFORMATION AND UPDATES
REGISTRATION LIST AND DISTRIBUTION KEY

S191: IS RECORDER UN-REGISTERABLE?

S192: RECEIVER AND RECORDER PERFORM MUTUAL AUTHENTICATION

S193: RECEIVER TRANSMITS REGISTRATION COMPLETION MESSAGE AND
DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND
RECORDER RECEIVES AND DECRYPTS REGISTRATION COMPLETION
MESSAGE AND DISTRIBUTION KEY

S194: RECORDER UPDATES DISTRIBUTION KEY

B: RETURN

FIG. 48

A: START PROCESSING OF RECEIVER FOR RECEIVING DISTRIBUTION
KEY

S201: RECEIVER MUTUALLY AUTHENTICATES WITH EMD SERVICE CENTER

S202: RECEIVER TRANSMITS CERTIFICATE TO EMD SERVICE CENTER

S203: IS RECEIVER UN-REGISTERABLE?

S204: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF
DISTRIBUTION KEY, CHARGING INFORMATION, HANDLING POLICY, AND
REGISTRATION LIST, WHICH HAVE BEEN ENCRYPTED BY USE OF
TEMPORARY KEY

S205: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, AND

PROCESSES CHARGING INFORMATION

S206: IS DISTRIBUTION KEY NEWEST VERSION?

S207: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S208: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST

S209: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY

S210: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY

B: RETURN

FIG. 49

A: START PROCESSING OF RECORDER FOR RECEIVING DISTRIBUTION KEY

S221: RECEIVER AND RECORDER PERFORM MUTUAL AUTHENTICATION

S222: IS RECORDER INCLUDED IN REGISTRATION LIST OF RECEIVER

S223: IS RECORDER UN-REGISTERABLE?

S224: RECORDER TRANSMITS TO RECEIVER VERSION OF DISTRIBUTION KEY AND CHARGING INFORMATION WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS VERSION OF DISTRIBUTION KEY AND CHARGING INFORMATION

S225: RECEIVER AND EMD SERVICE CENTER PERFORM MUTUAL AUTHENTICATION

S226: IS RECEIVER UN-REGISTERABLE?

S227: RECEIVER TRANSMITS TO EMD SERVICE CENTER VERSION OF DISTRIBUTION KEY, CHARGING INFORMATION, HANDLING POLICY, AND REGISTRATION LIST OF RECEIVER, AS WELL AS CHARGING INFORMATION OF RECORDER, WHICH HAVE BEEN ENCRYPTED BY USE OF TEMPORARY KEY

S228: EMD SERVICE CENTER DECRYPTS RECEIVED DATA, AND PROCESSES CHARGING INFORMATION

S229: IS DISTRIBUTION KEY OF RECEIVER NEWEST VERSION?

S230: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST AND CHARGING-INFORMATION RECEIPT MESSAGE

S231: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST

S232: EMD SERVICE CENTER TRANSMITS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND RECEIVER RECEIVES AND DECRYPTS REGISTRATION LIST, CHARGING-INFORMATION RECEIPT MESSAGE, AND DISTRIBUTION KEY

S233: RECEIVER ERASES CHARGING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY

S234: IS RECORDER UN-REGISTERABLE?

S235: RECEIVER TRANSMITS CHARGING-INFORMATION RECEIPT MESSAGE AND DISTRIBUTION KEY ENCRYPTED BY USE OF TEMPORARY KEY, AND

RECORDER RECEIVES AND DECRYPTS CHARGING-INFORMATION RECEIPT
MESSAGE AND DISTRIBUTION KEY

S236: RECORDER ERASES CHARGING INFORMATION AND UPDATES
DISTRIBUTION KEY

S237: REGISTER RECORDER

B: RETURN

FIG. 50

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO
SERVICE PROVIDER

S251: INSERT WATERMARK INTO CONTENT

S252: COMPRESS CONTENT

S253: GENERATE RANDOM NUMBER AS CONTENT KEY

S254: ENCRYPT CONTENT BY USE OF CONTENT KEY

S255: ENCRYPT CONTENT KEY BY USE OF DISTRIBUTION KEY

S256: CREATE SIGNATURE

S257: CREATE SECURE CONTAINER

S258: MUTUALLY AUTHENTICATE WITH SERVICE PROVIDER

S259: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 51

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO
SERVICE PROVIDER

S271: INSERT WATERMARK INTO CONTENT

S272: COMPRESS CONTENT

S273: GENERATE RANDOM NUMBER AS CONTENT KEY
S274: ENCRYPT CONTENT BY USE OF CONTENT KEY
S275: ENCRYPT CONTENT KEY AND HANDLING POLICY BY USE OF
DISTRIBUTION KEY
S276: CREATE SIGNATURE
S277: CREATE SECURE CONTAINER
S278: MUTUALLY AUTHENTICATE WITH SERVICE PROVIDER
S279: TRANSMIT SECURE CONTAINER
B: RETURN

FIG. 52

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO
RECEIVER
S291: EXTRACT PUBLIC KEY FROM CERTIFICATE OF SECURE CONTAINER
S292: CONFIRM THAT SECURE CONTAINER HAS NOT BEEN TAMPERED
S293: EXTRACT HANDLING POLICY FROM SECURE CONTAINER
S294: PRODUCE PRICE INFORMATION
S295: CREATE SECURE CONTAINER
S296: MUTUALLY AUTHENTICATE WITH RECEIVER
S299: TRANSMIT SECURE CONTAINER
B: RETURN

FIG. 53

A: START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO
RECEIVER
S311: EXTRACT PUBLIC KEY FROM CERTIFICATE OF SECURE CONTAINER
S312: CONFIRM THAT SECURE CONTAINER HAS NOT BEEN TAMPERED

S313: DECRYPTS HANDLING POLICY OF SECURE CONTAINER BY USE OF
DISTRIBUTION KEY

S314: PRODUCE HANDLING CONTROL INFORMATION

S315: PRODUCE PRICE INFORMATION

S316: CREATE SECURE CONTAINER

S317: MUTUALLY AUTHENTICATE WITH RECEIVER

S318: TRANSMIT SECURE CONTAINER

B: RETURN

FIG. 54

A: START CHARGING PROCESSING

S331: CAN CONTENT KEY BE DECRYPTED BY USE OF DISTRIBUTION
KEY?

S332: PROCESSING FOR RECEIVING DISTRIBUTION KEY

S333: DECRYPTS CONTENT KEY BY USE OF DISTRIBUTION KEY?

S334: PRODUCE CHARGING INFORMATION AND CONDITIONS-FOR-USE
FROM HANDLING POLICY AND PRICE INFORMATION

S335: IS TOTAL OF CHARGES UPPER LIMIT?

S336: PROCESSING FOR RECEIVING DISTRIBUTION KEY

S337: STORE CHARGING INFORMATION IN SAM

S338: RECORD CONDITIONS-FOR-USE INFORMATION IN HDD

S339: RECORD HANDLING POLICY IN HDD

S340: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S341: STORE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION IN
SAM

S342: GENERATE RANDOM NUMBER AS SAVE KEY

S343: ENCRYPT CONTENT KEY BY USE OF SAVE KEY

S344: RECORD CONTENT KEY IN HDD

S345: STORE SAVE KEY IN SAM

B: RETURN

FIG. 55

A: START REPRODUCTION PROCESSING

S361: READ CONDITIONS-FOR-USE INFORMATION AND CONTENT KEY
FROM HDD

S362: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S363: COINCIDE WITH HASH VALUE WITHIN SAM?

S364: UPDATE CONDITIONS-FOR-USE INFORMATION

S365: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S366: STORE HASH VALUE IN SAM

S367: STORE CONDITIONS-FOR-USE INFORMATION IN HDD

S368: SAM AND EXTENSION SECTION PERFORM MUTUAL AUTHENTICATION
AND SHARE TEMPORARY KEY

S369: DECRYPT CONTENT KEY BY USE OF SAVE KEY

S370: ENCRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S371: TRANSMIT CONTENT KEY TO EXTENSION SECTION

S372: DECRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S373: TRANSMIT CONTENT TO EXTENSION SECTION

S374: DECRYPT CONTENT BY USE OF CONTENT KEY

S375: EXTEND CONTENT

S376: ADD WATERMARK TO CONTENT

S377: OUTPUT CONTENT

S378: ERROR PROCESSING

B: RETURN

FIG. 56

A: START REPRODUCTION PROCESSING

S391: READ CONDITIONS-FOR-USE INFORMATION AND CONTENT KEY
FROM HDD

S392: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S393: COINCIDE WITH HASH VALUE WITHIN SAM?

S394: UPDATE CONDITIONS-FOR-USE INFORMATION

S395: CALCULATE HASH VALUE OF CONDITIONS-FOR-USE INFORMATION

S396: STORE HASH VALUE IN SAM

S397: STORE CONDITIONS-FOR-USE INFORMATION IN HDD

S398: SAM AND DECODER PERFORM MUTUAL AUTHENTICATION AND SHARE
TEMPORARY KEY

S399: DECRYPT CONTENT KEY BY USE OF SAVE KEY

S400: ENCRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S401: TRANSMIT CONTENT KEY TO DECODER

S402: DECRYPT CONTENT KEY BY USE OF TEMPORARY KEY

S403: TRANSMIT CONTENT TO DECODER

S404: DECRYPT CONTENT BY USE OF CONTENT KEY

S405: EXTEND CONTENT

S406: ADD WATERMARK TO CONTENT

S407: OUTPUT CONTENT

S408: ERROR PROCESSING

B: RETURN

FIG. 57

A: START PROCESSING FOR PRODUCING SETTLEMENT OBJECTS

S421: SELECT CHARGING INFORMATION REGARDING USE OF CERTAIN
CONTENT

S422: DOES CHARGING INFORMATION INCLUDE PROFIT DISTRIBUTION
TO CONTENT PROVIDER AND SERVICE PROVIDER?

S423: CALCULATE AMOUNT WHICH USER MUST PAY TO SERVICE
PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF CHARGING
INFORMATION

S424: CALCULATE AMOUNT WHICH SERVICE PROVIDER MUST PAY TO
CONTENT PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF
CHARGING INFORMATION

S425: CALCULATE AMOUNT WHICH CONTENT PROVIDER MUST PAY TO
PROPRIETARY ORGANIZATION WITH REFERENCE TO PROFIT
DISTRIBUTION OF CHARGING INFORMATION

S426: CALCULATE AMOUNT WHICH USER MUST PAY TO SERVICE
PROVIDER WITH REFERENCE TO PROFIT-DISTRIBUTION DATA BASE

S427: CALCULATE AMOUNT WHICH SERVICE PROVIDER MUST PAY TO
CONTENT PROVIDER WITH REFERENCE TO PROFIT-DISTRIBUTION DATA
BASE

S428: CALCULATE AMOUNT WHICH CONTENT PROVIDER MUST PAY TO
PROPRIETARY ORGANIZATION WITH REFERENCE TO PROFIT-
DISTRIBUTION DATA BASE

S429: CORRECT INDIVIDUAL PAYMENT AMOUNTS WITH REFERENCE TO
DISCOUNT INFORMATION DATA BASE

S430: HAS CALCULATION BEEN PERFORMED FOR ALL CONTENTS?

S431: CALCULATE AMOUNT WHICH USER MUST PAY TO EACH SERVICE
PROVIDER AND PRODUCE SETTLEMENT OBJECT 1

S432: CALCULATE AMOUNT WHICH EACH SERVICE PROVIDER MUST PAY

TO EACH CONTENT PROVIDER AND PRODUCE SETTLEMENT OBJECT 2
S433: CALCULATE AMOUNT WHICH EACH CONTENT PROVIDER MUST PAY
TO PROPRIETARY ORGANIZATION AND PRODUCE SETTLEMENT OBJECT 3
S434: DETERMINE AMOUNT TO BE COLLECTED FROM USER, WITH
REFERENCE TO SERVICE CHARGE OF EMD SERVICE CENTER AND PRODUCE
SETTLEMENT OBJECT 4

B: END

FIG. 58

A:

CREDIT SETTLEMENT

OBJECT 1

PAYER: ID OF USER

COLLECTION AMOUNT: x

RECEIVER: ID OF SERVICE PROVIDER

PAYMENT AMOUNT: x1

B:

CREDIT SETTLEMENT

OBJECT 2

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF CONTENT PROVIDER

PAYMENT AMOUNT: x2

C :

CREDIT SETTLEMENT

OBJECT 3

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF PROPRIETARY ORGANIZATION

PAYMENT AMOUNT: x3

D :

CREDIT SETTLEMENT

OBJECT 4

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: x4

FIG. 59

A:

BANK SETTLEMENT

OBJECT 1

PAYER: ID OF SERVICE PROVIDER

COLLECTION AMOUNT: y1

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y1

B:

BANK SETTLEMENT

OBJECT 2

PAYER: ID OF CONTENT PROVIDER

COLLECTION AMOUNT: y2

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y2

C:

BANK SETTLEMENT

OBJECT 3

PAYER: ID OF PROPRIETARY ORGANIZATION

COLLECTION AMOUNT: y_3

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: y_3

FIG. 60

A:

CREDIT SETTLEMENT

OBJECT 1

PAYER: ID OF USER

COLLECTION AMOUNT: x

RECEIVER: ID OF SERVICE PROVIDER

PAYMENT AMOUNT: x_1

B:

BANK SETTLEMENT

OBJECT 2

PAYER: ID OF SERVICE PROVIDER

COLLECTION AMOUNT: $x_2 + x_3$

RECEIVER: ID OF CONTENT PROVIDER

PAYMENT AMOUNT: $x_2 + x_3$

C:

BANK SETTLEMENT

OBJECT 3

PAYER: ID OF CONTENT PROVIDER

COLLECTION AMOUNT: x_3

RECEIVER: ID OF PROPRIETARY ORGANIZATION

PAYMENT AMOUNT: x3

D :

CREDIT SETTLEMENT

OBJECT 4

PAYER: CREDIT SETTLEMENT OBJECT 1

COLLECTION AMOUNT: -

RECEIVER: ID OF EMD SERVICE CENTER

PAYMENT AMOUNT: x4

FIG. 61

A: START CREDIT SETTLEMENT PROCESSING

S451: OBTAIN SETTLEMENT INSTITUTE OF RECEIVER FROM RECEIVER
ID

S452: OBTAIN SETTLEMENT INSTITUTE OF PAYER FROM PAYER ID

S453: IS CREDIT-CHECK PROCESSING NECESSARY?

S454: EXECUTE CREDIT-CHECK PROCESSING

S455: HAS PREVIOUSLY-EXECUTED SETTLEMENT OBJECT PROCESSING
ENDED?

S456: TRANSMIT SETTLEMENT INSTRUCTIONS TO SETTLEMENT
INSTITUTES

S457: TRANSMIT SETTLEMENT INFORMATION TO RECEIVER

S458: TRANSMIT SETTLEMENT INFORMATION TO PAYER

S459: EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT

B: END

FIG. 62

A: START BANK SETTLEMENT PROCESSING

S471: OBTAIN SETTLEMENT INSTITUTE OF RECEIVER FROM RECEIVER
ID

S472: OBTAIN SETTLEMENT INSTITUTE OF PAYER FROM PAYER ID

S473: HAS PREVIOUSLY-EXECUTED SETTLEMENT OBJECT PROCESSING
ENDED?

S474: TRANSMIT SETTLEMENT INSTRUCTIONS TO SETTLEMENT
INSTITUTES

S475: TRANSMIT SETTLEMENT INFORMATION TO RECEIVER

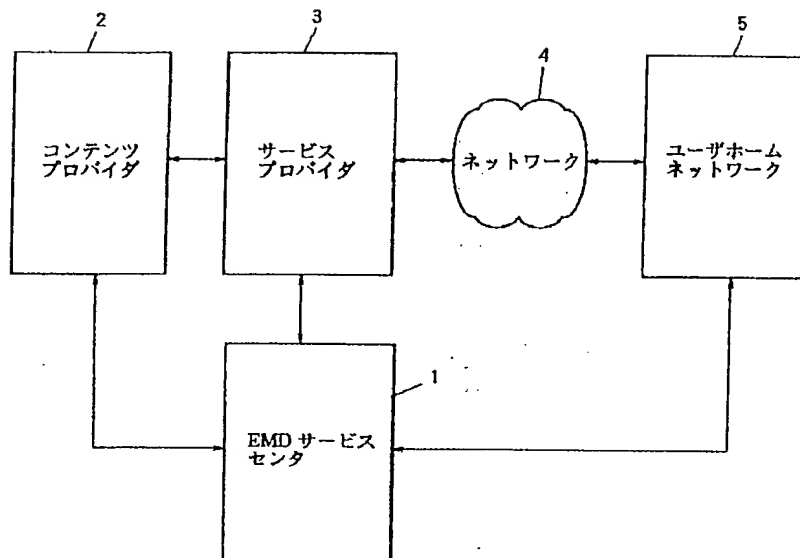
S476: TRANSMIT SETTLEMENT INFORMATION TO PAYER

S477: EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT

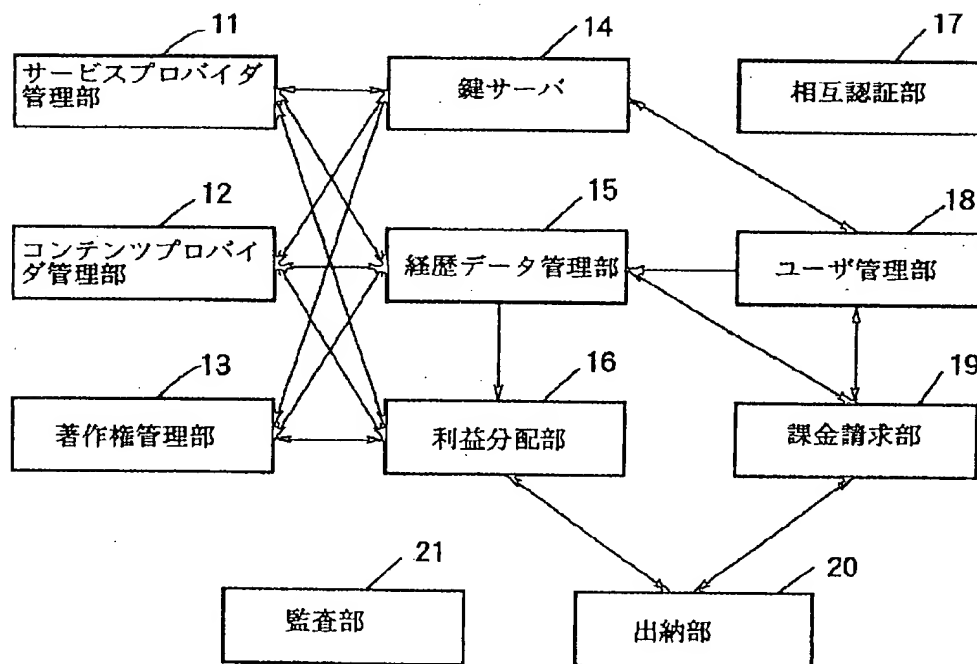
B: END

THIS PAGE BLANK (USPTO)

【図 1】

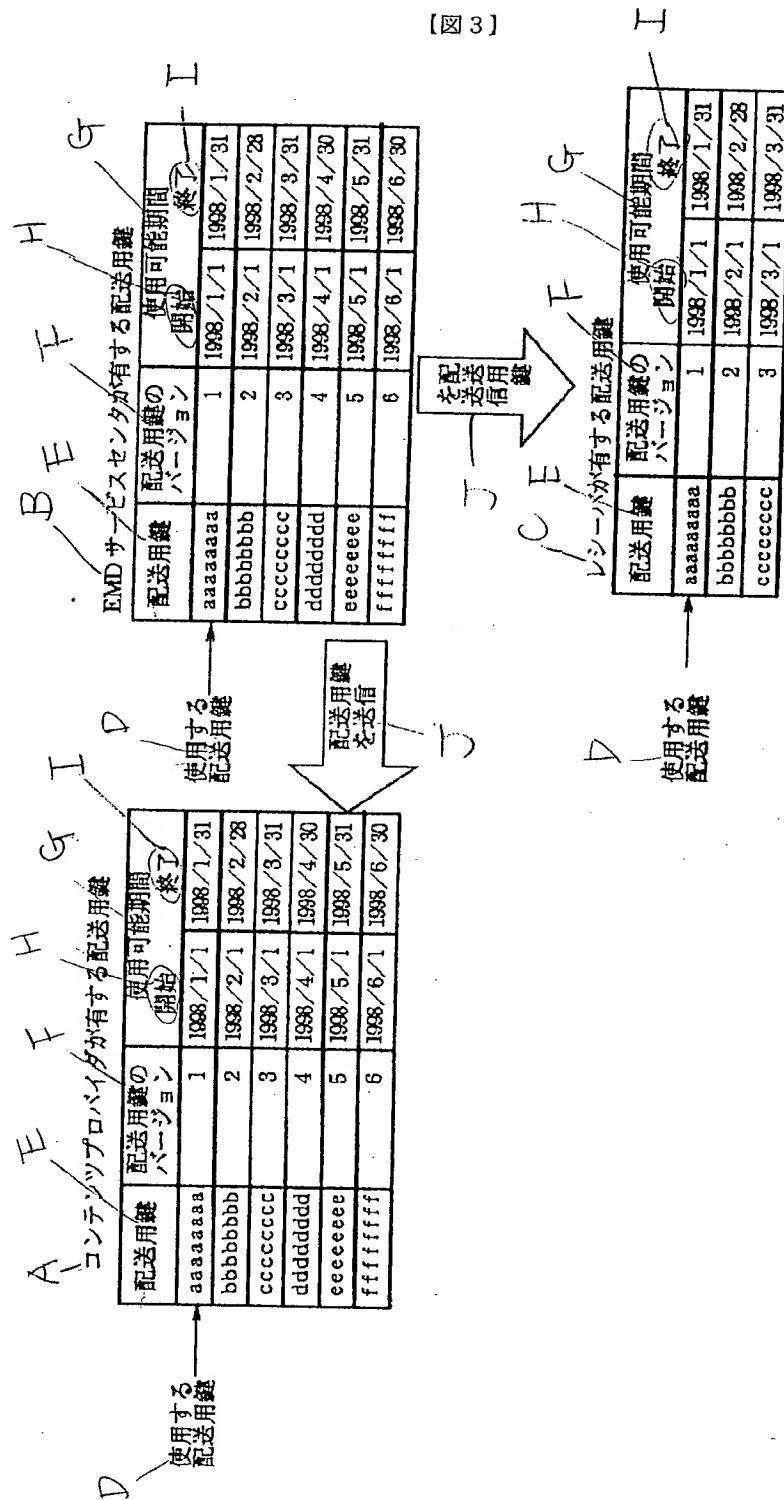


【図 2】



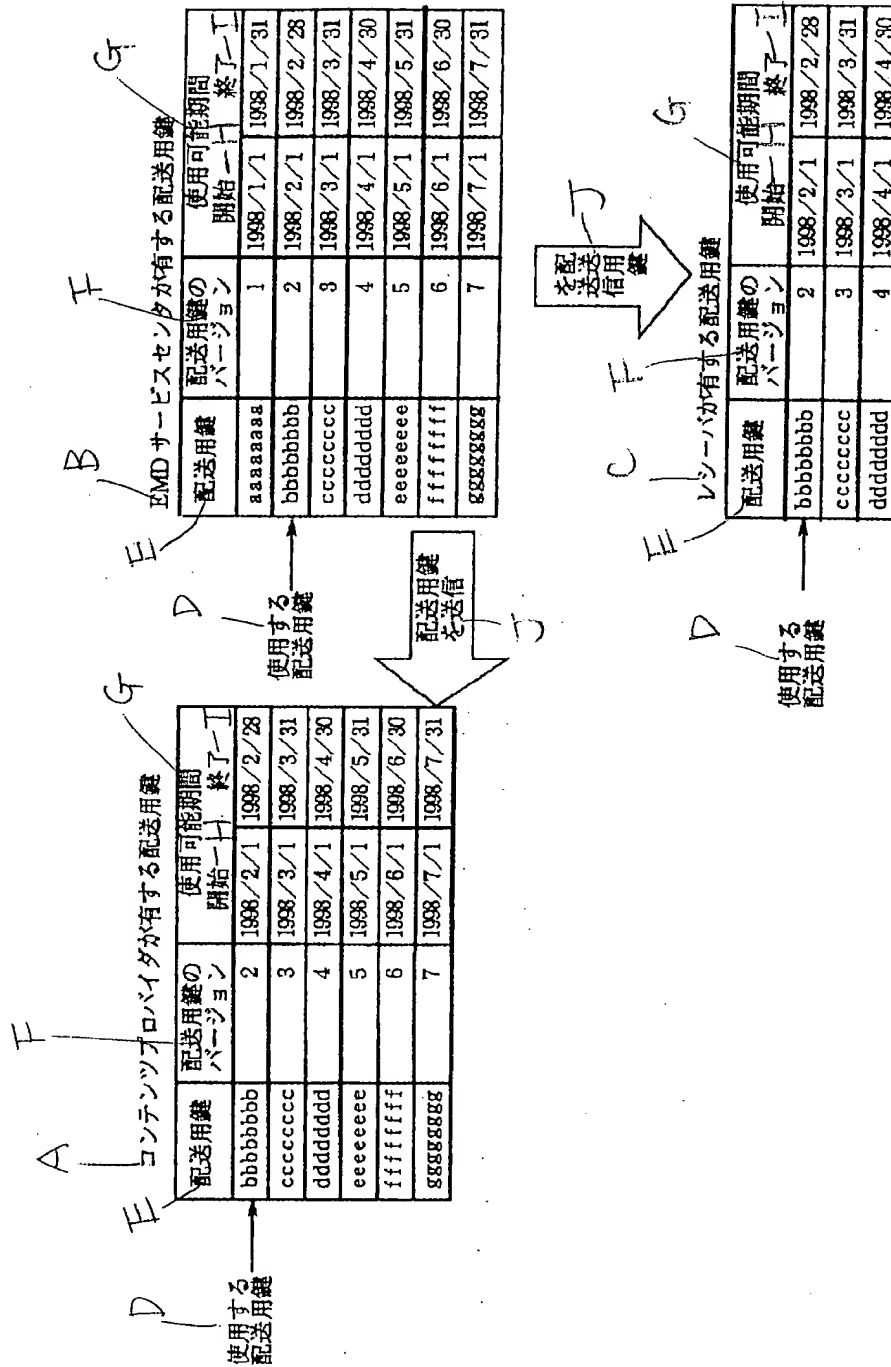
A — EMD サービスセンタ 1

【図 3】



[図 4]

Fig. 3 と同じ



【図 5】

Fig. 3 と同じ

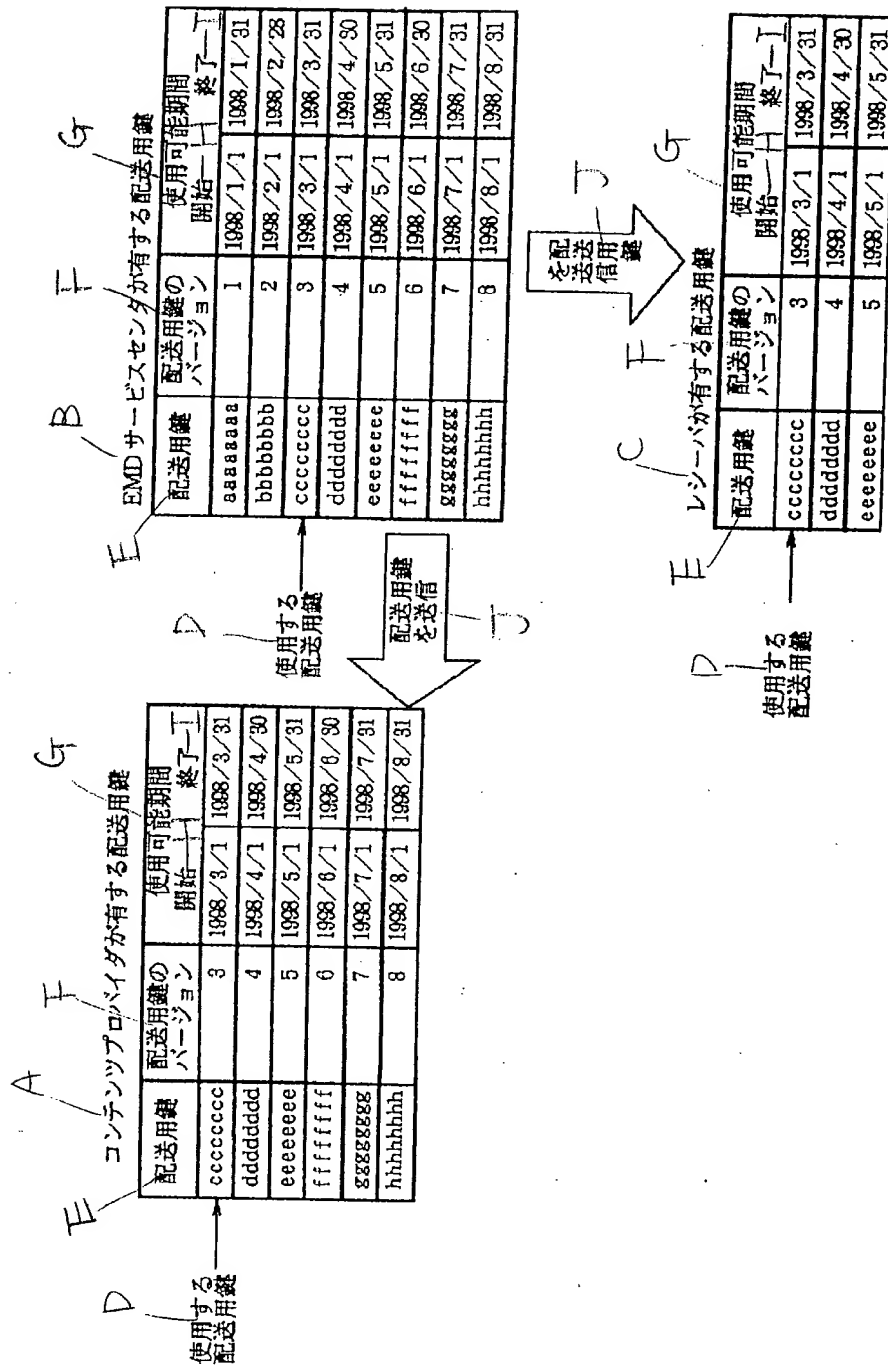
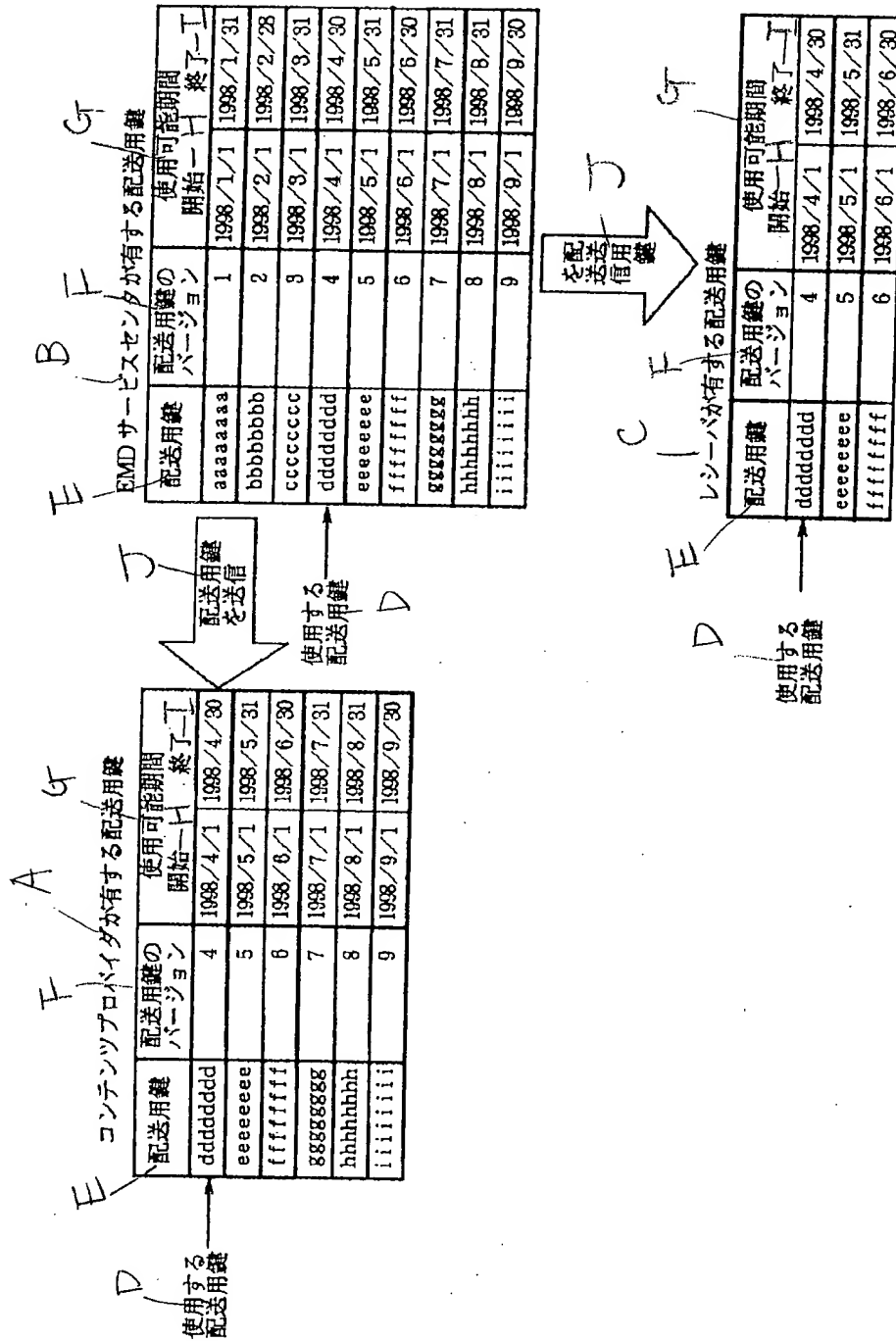


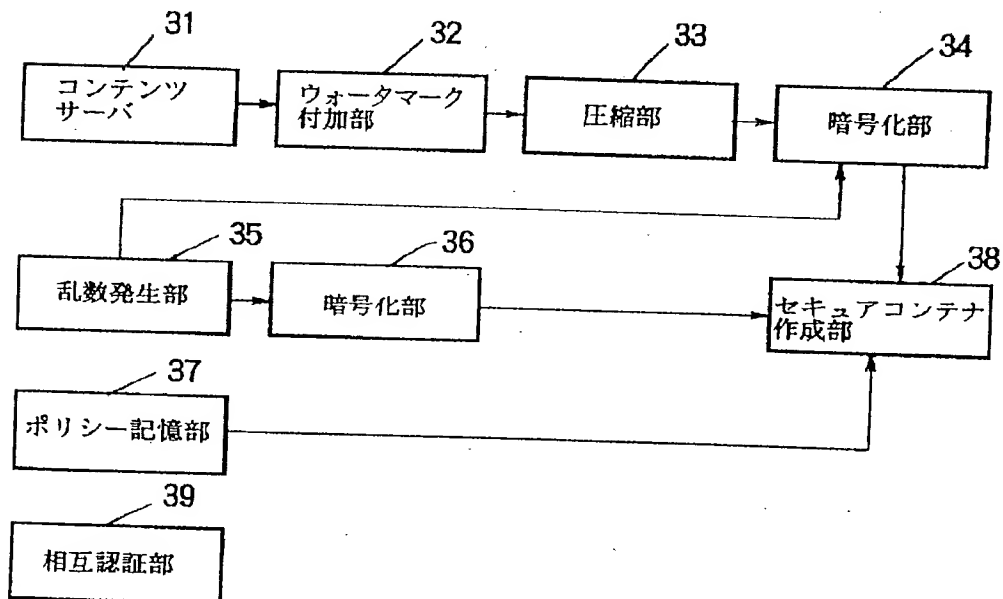
Fig. 3 & 10



(図 7)

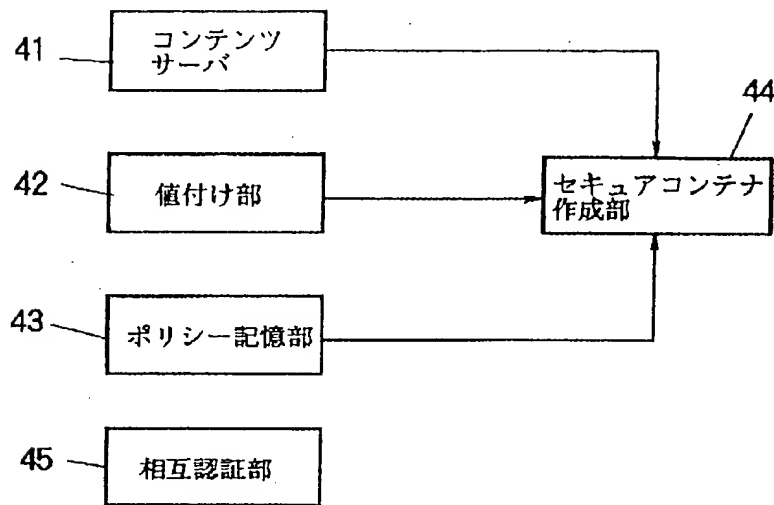
ID	決済処理	登録	EMDサービスセンタとの接続
0000000000000001h	可	可	可
0000000000000002h	可	可	不可
0000000000000003h	可	不可	可
0000000000000004h	可	不可	不可
0000000000000005h	不可	可	可
0000000000000006h	不可	可	不可
0000000000000007h	不可	不可	可
0000000000000008h	不可	不可	不可
0000000000000009h	可	可	可
...			
FFFFFFFFFFFFFFFeh	可	不可	不可
FFFFFFFFFFFFFFFfh	不可	可	可

(図 8)



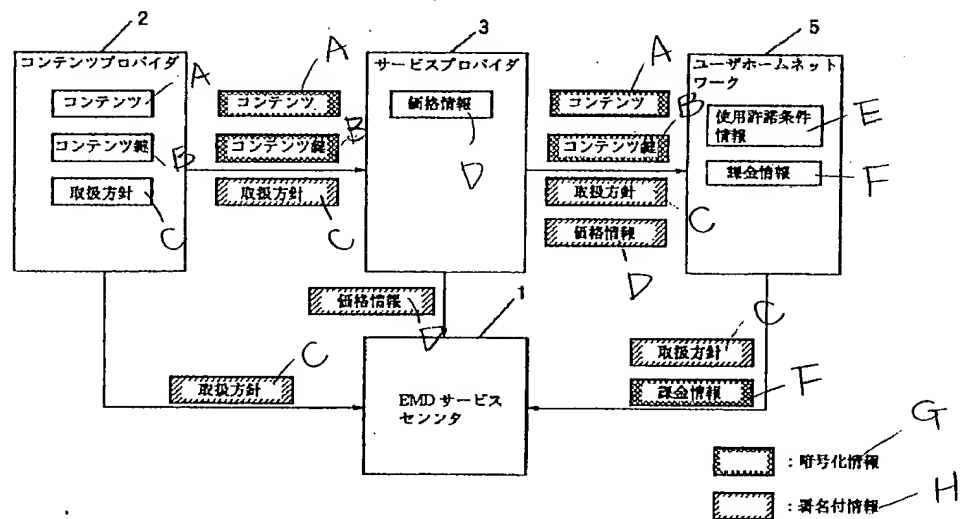
A — コンテンツプロバイダ 2

【図 9】



サービスプロバイダ 3 - A

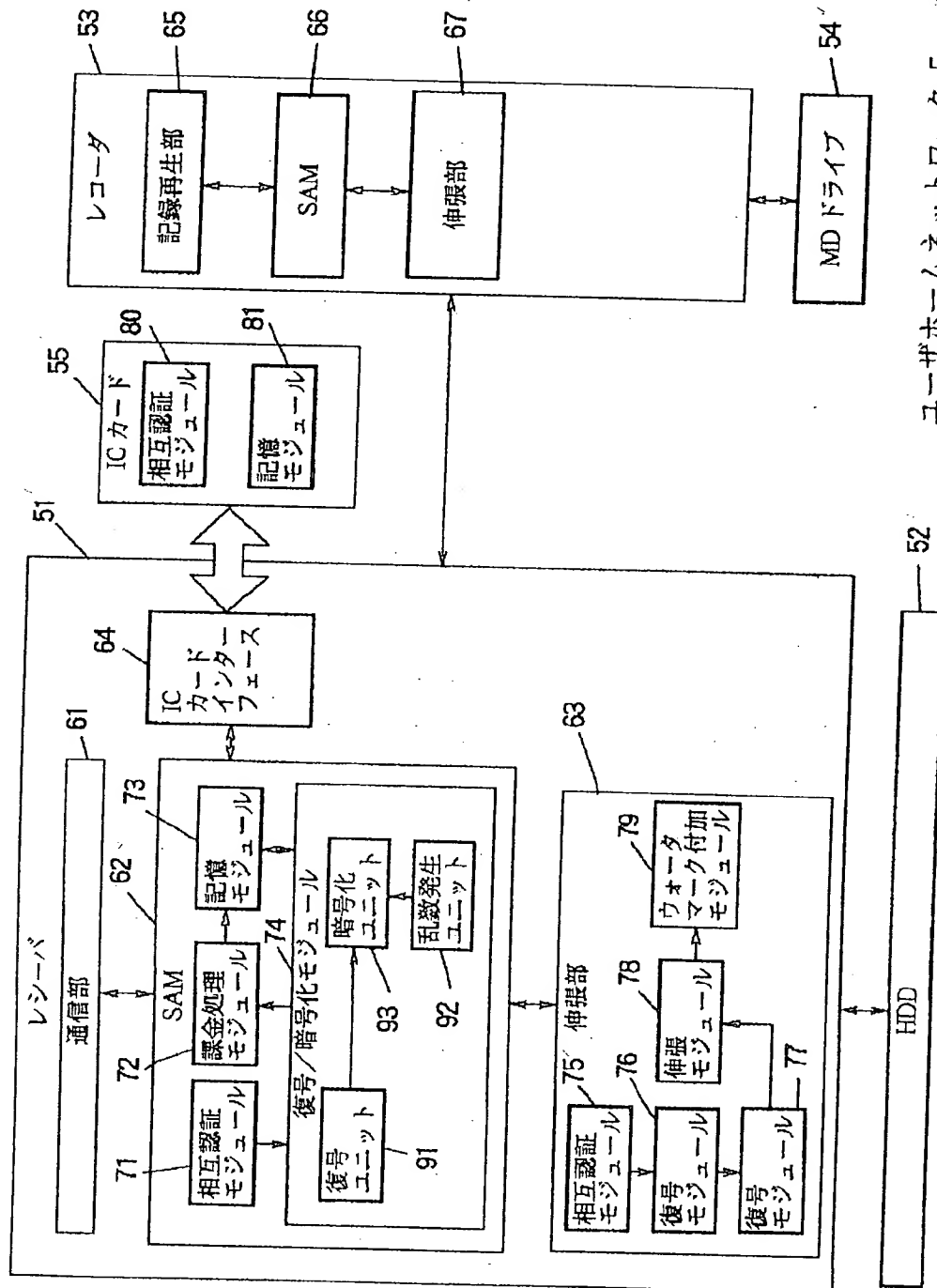
【図 12】



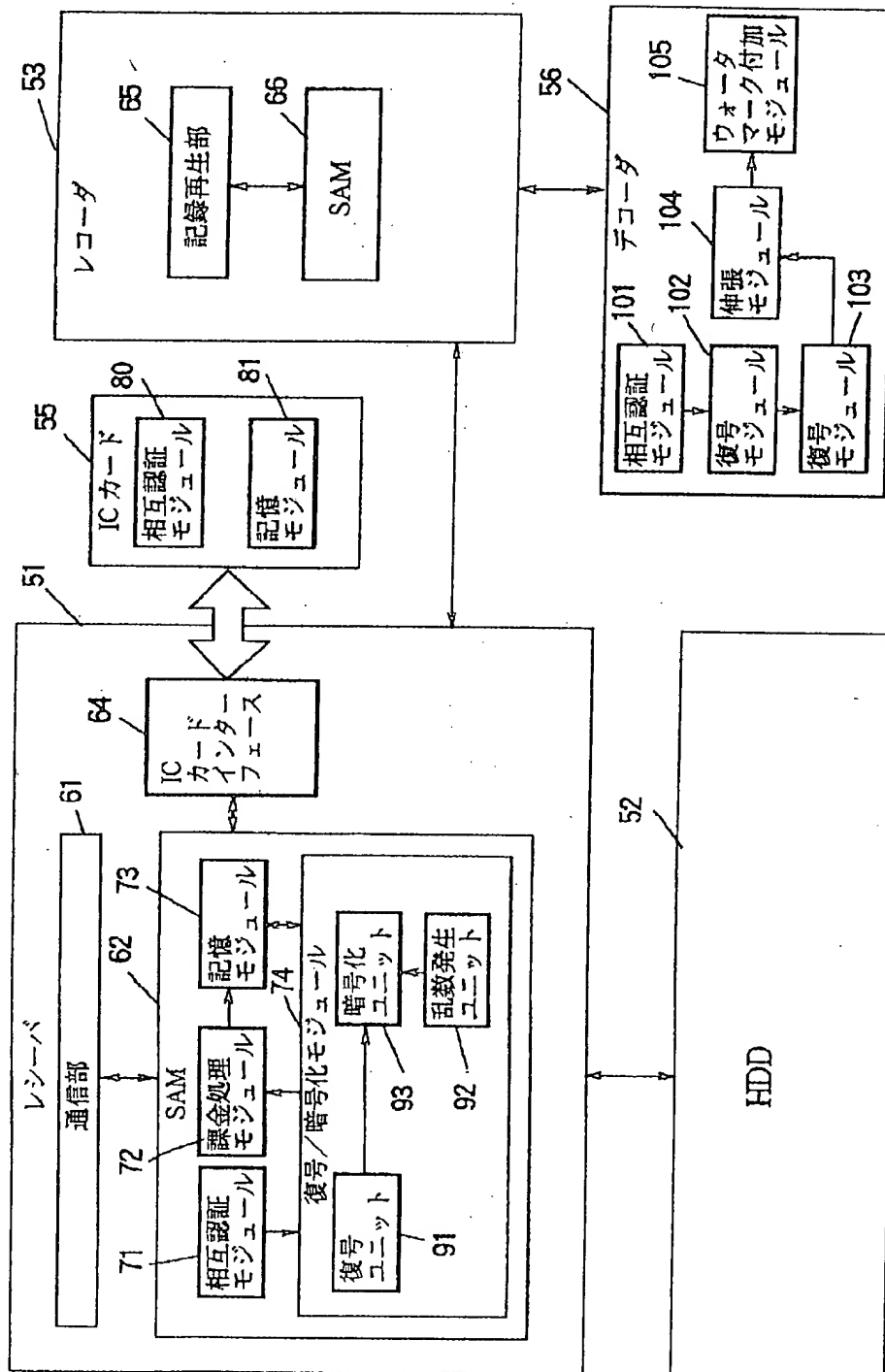
【図 28】

コンテンツ ID	コンテンツプロバイダ ID	権利団体
1	201	10%
2	201	20%

ユーザホームネットワーク5-A

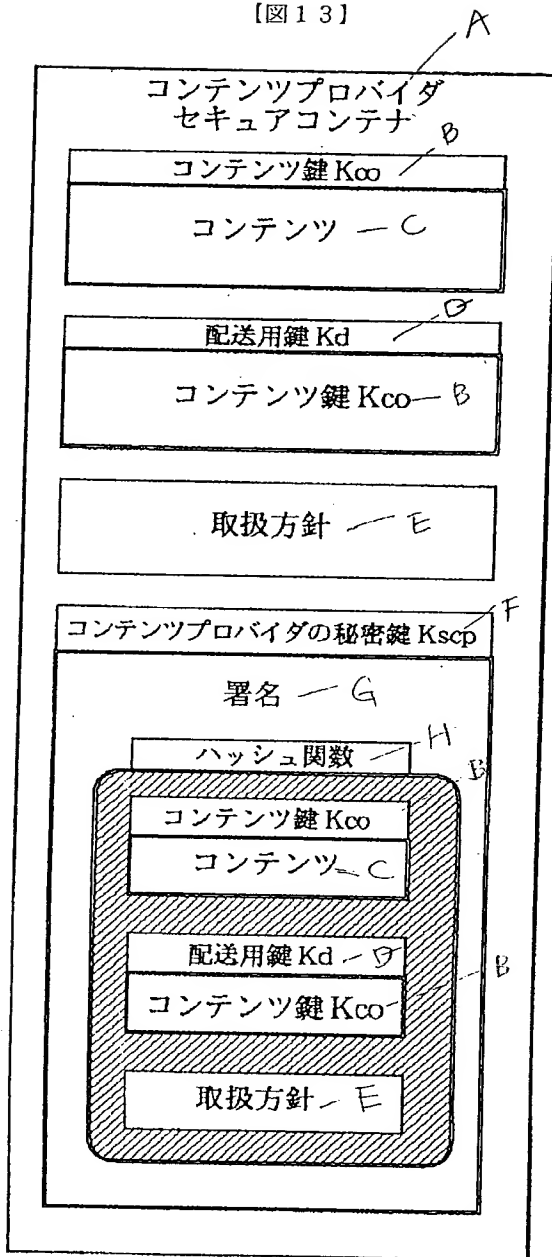


【図 11】

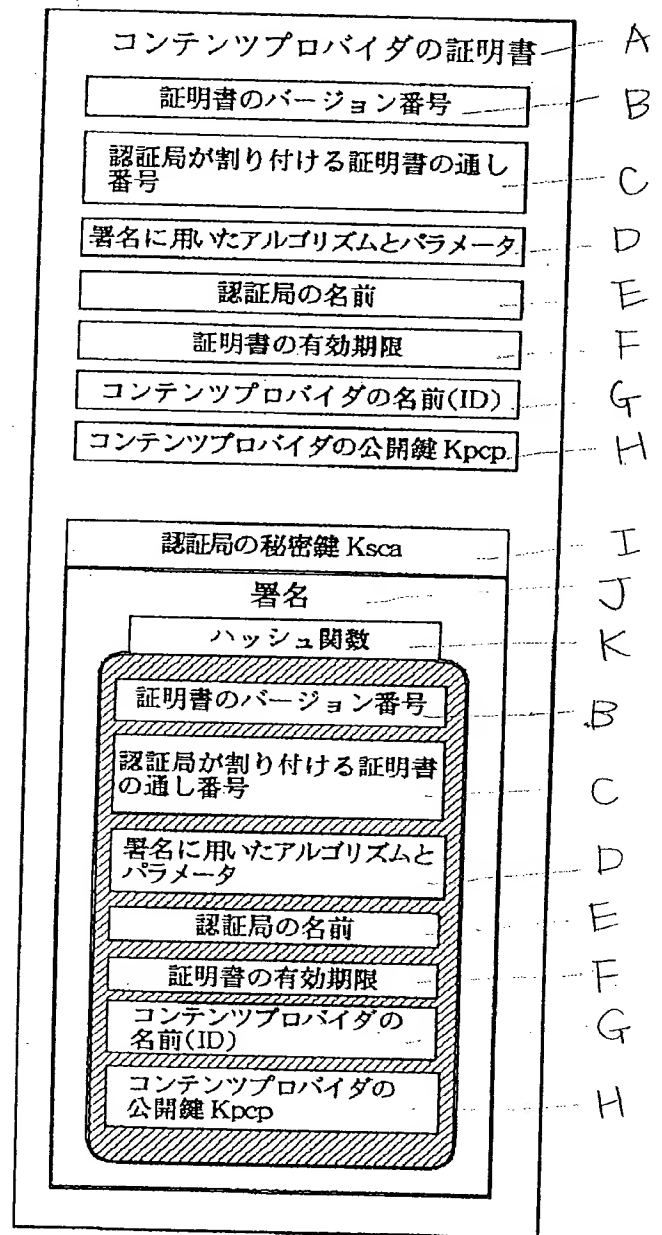


ユーザホームネットワーク 5—A

【図 13】



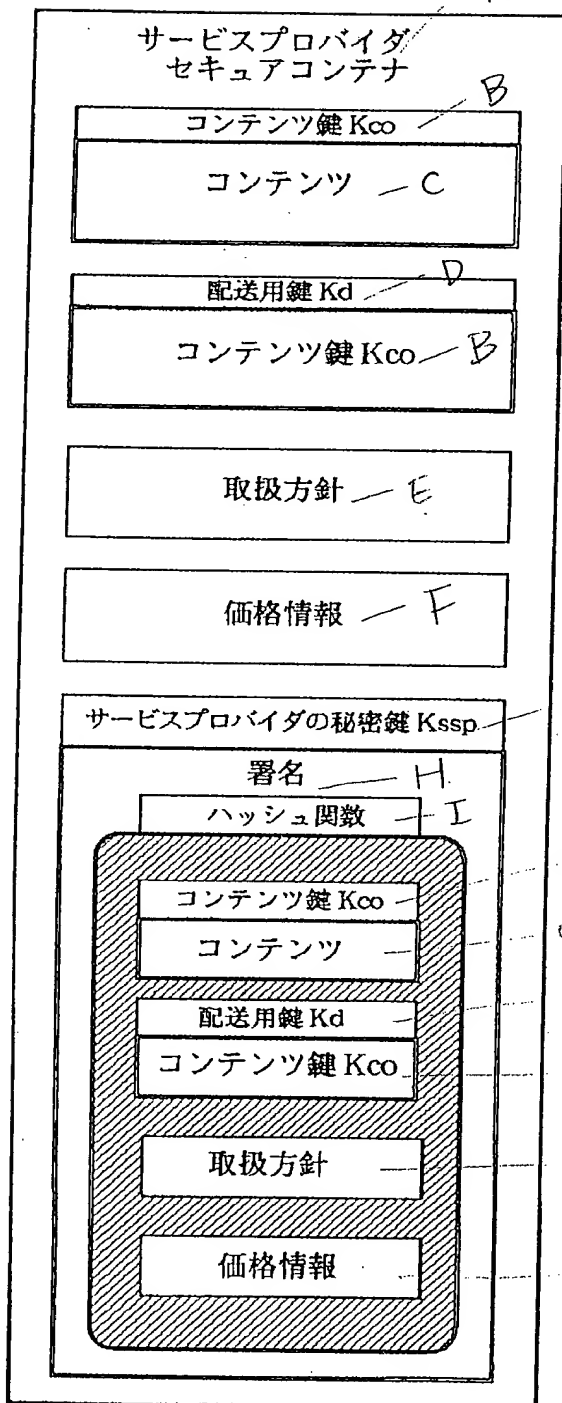
【図 14】



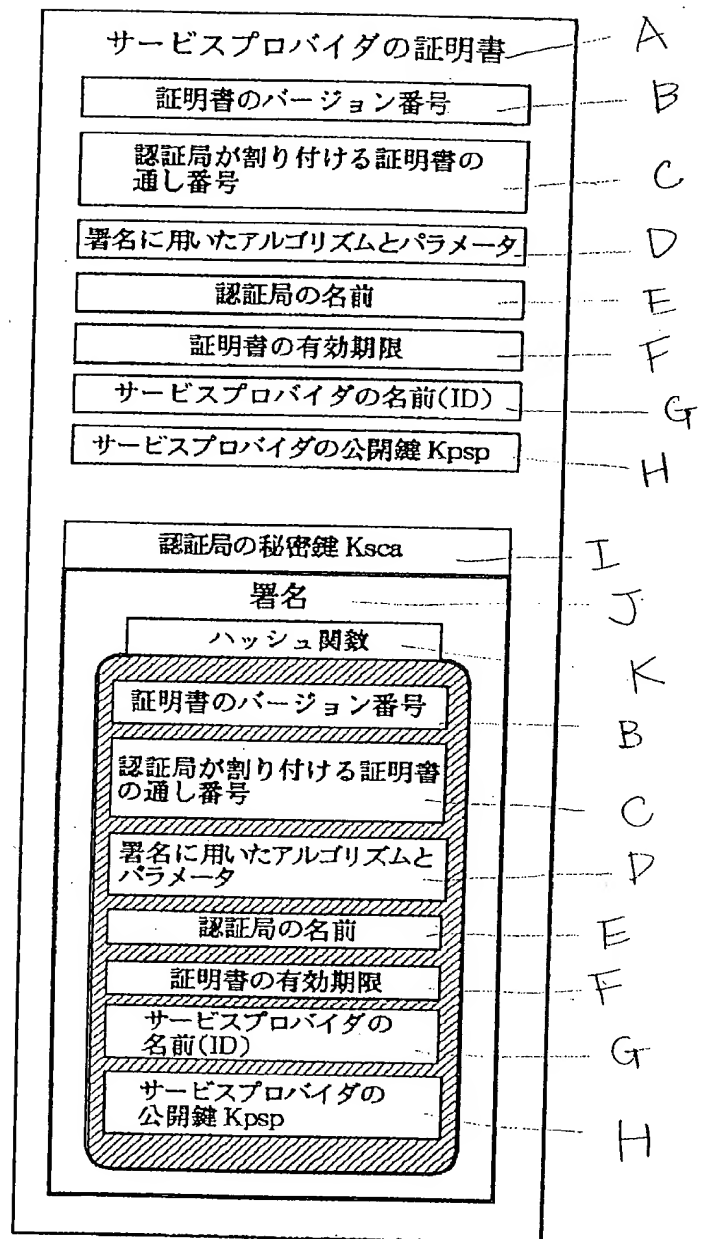
【図 29】

プロバイダ ID	コンテンツ ID	割引率	期間
コンテンツプロバイダ 1	1	0.02	1998.9~1998.12
	2	0.03	
	すべてのコンテンツ	0.01	
コンテンツプロバイダ 2	3	0.05	
サービスプロバイダ 1	1	0.03	
サービスプロバイダ 2	4	0.01	

【図 15】

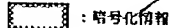
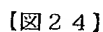
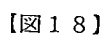


【図 1.6】



【図 30】

月額固定額	変動額		
	期間	1998. 8. ~ 1998. 9	- 10%
1000 円	利用料	3000 円以上	- 5%



クレジット決済
オブジェクト

(A)

クレジット決済
オブジェクト2

(B)

クレジット決済
オブジェクト3

(C)

クレジット決済
オブジェクト4

(D)

銀行決済
オブジェクト 1

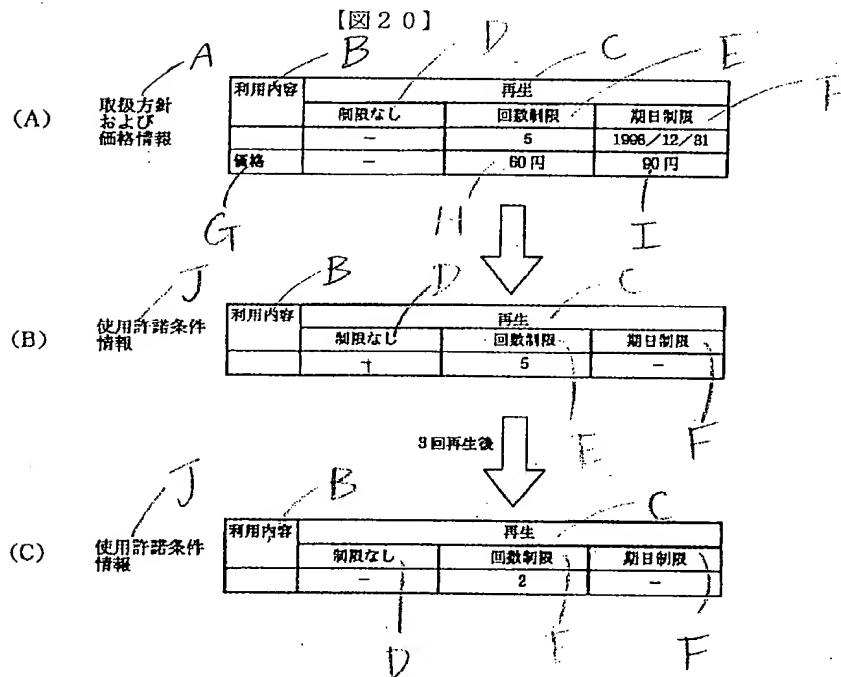
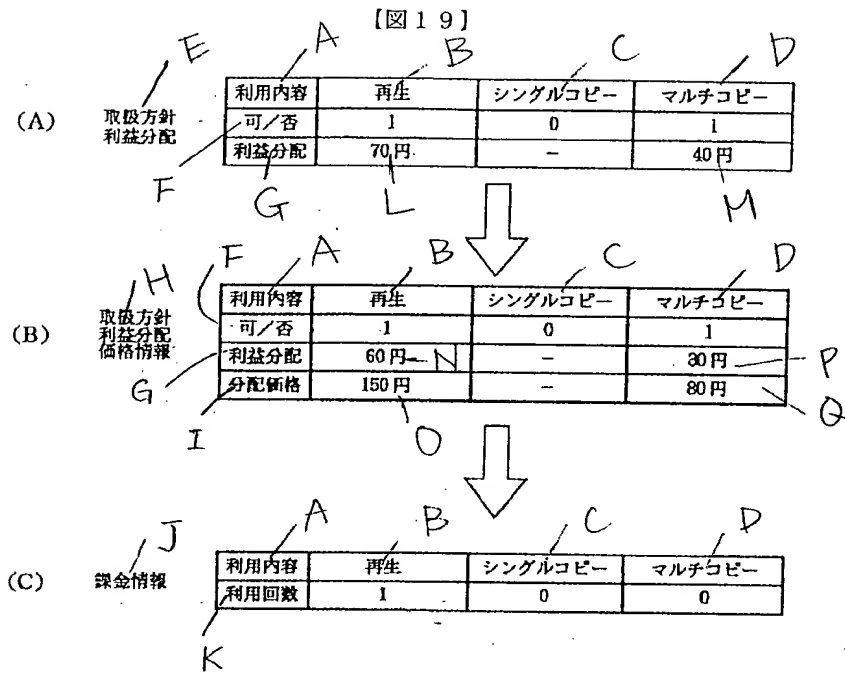
(A)

銀行決済
オブジェクト 2

(B)

銀行決済
オブジェクト3

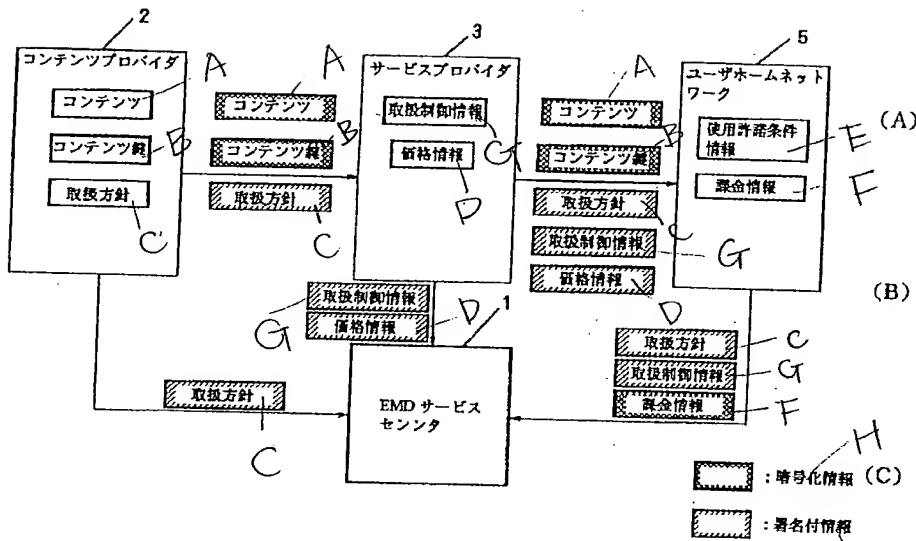
...



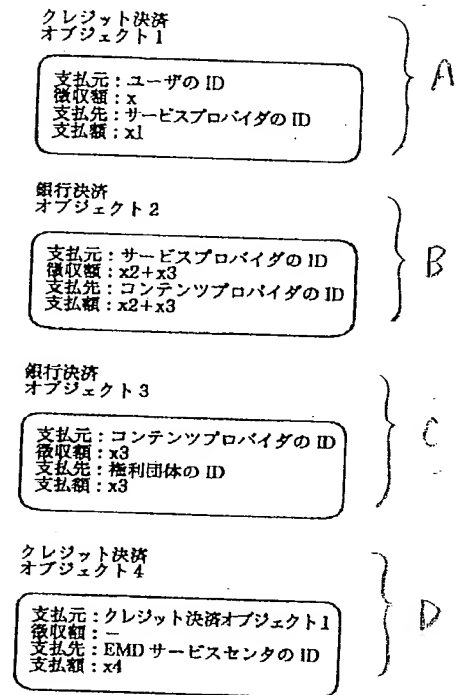
【図42】

SAMのID (64bit)	登録拒絶フラグ (1bit)	ステータスフラグ (4bit)	コンディションフラグ (1bit)	署名
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

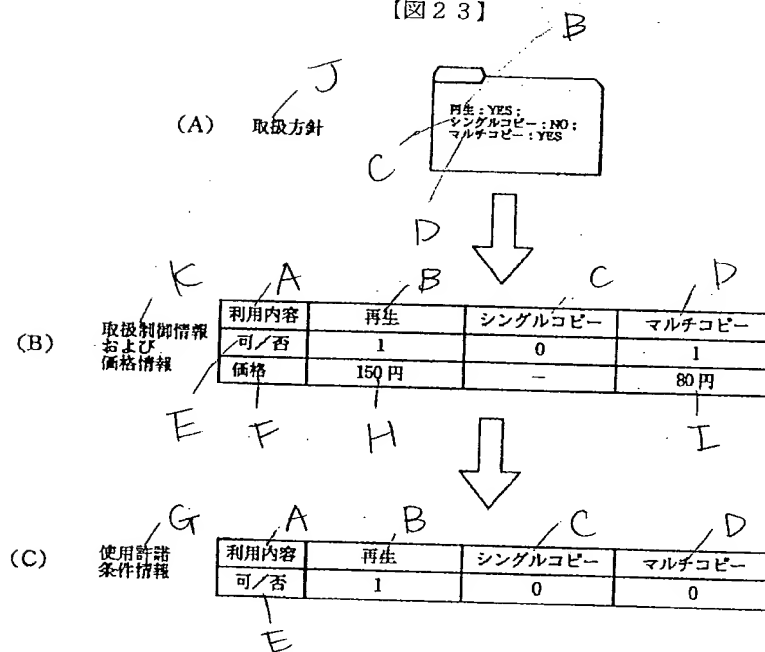
【図 21】



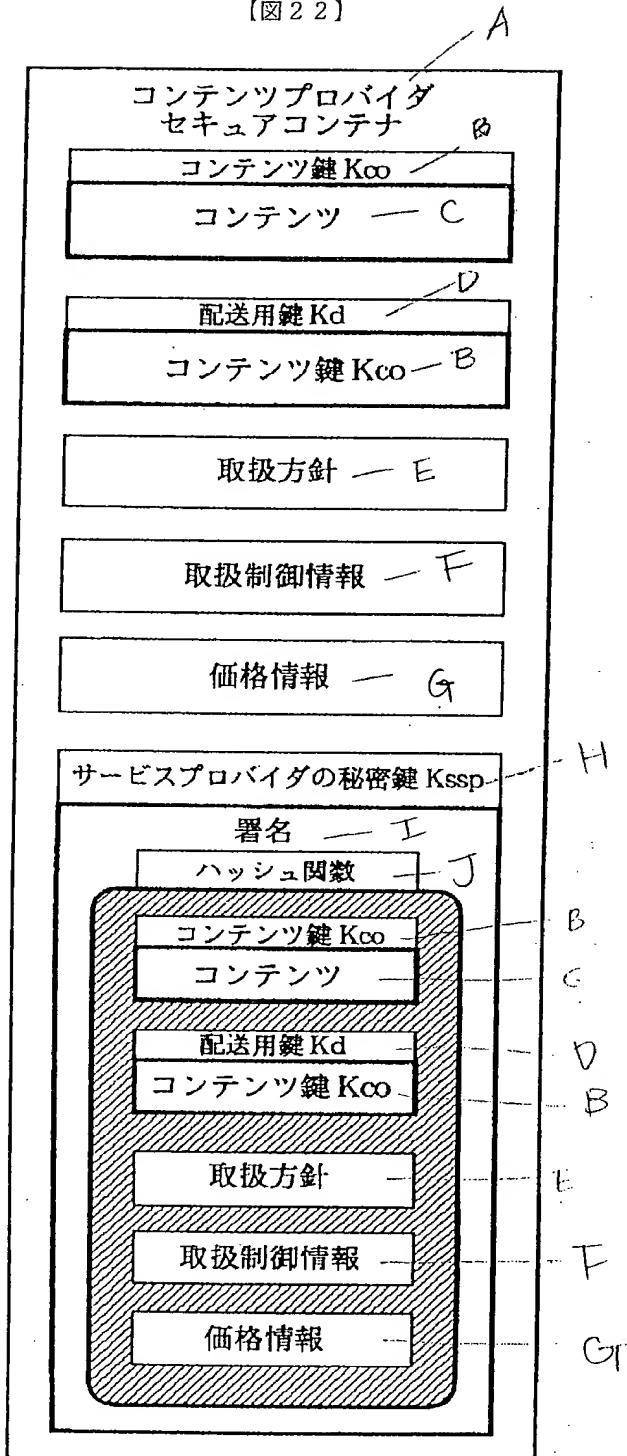
【図 60】



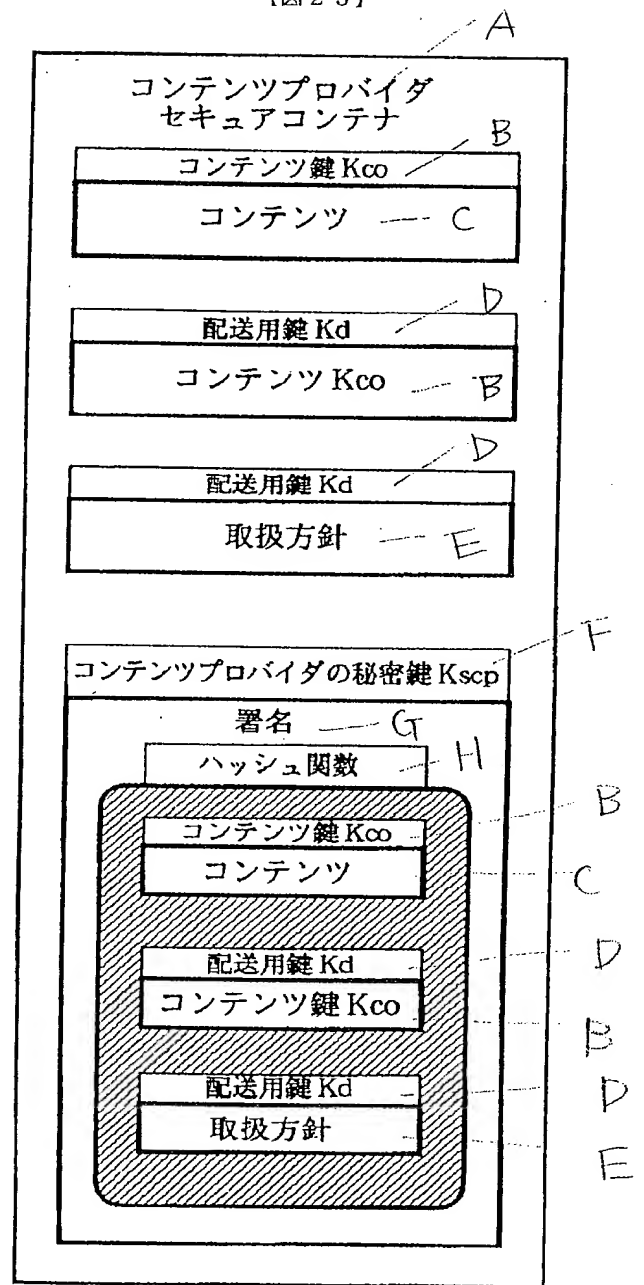
【図 23】



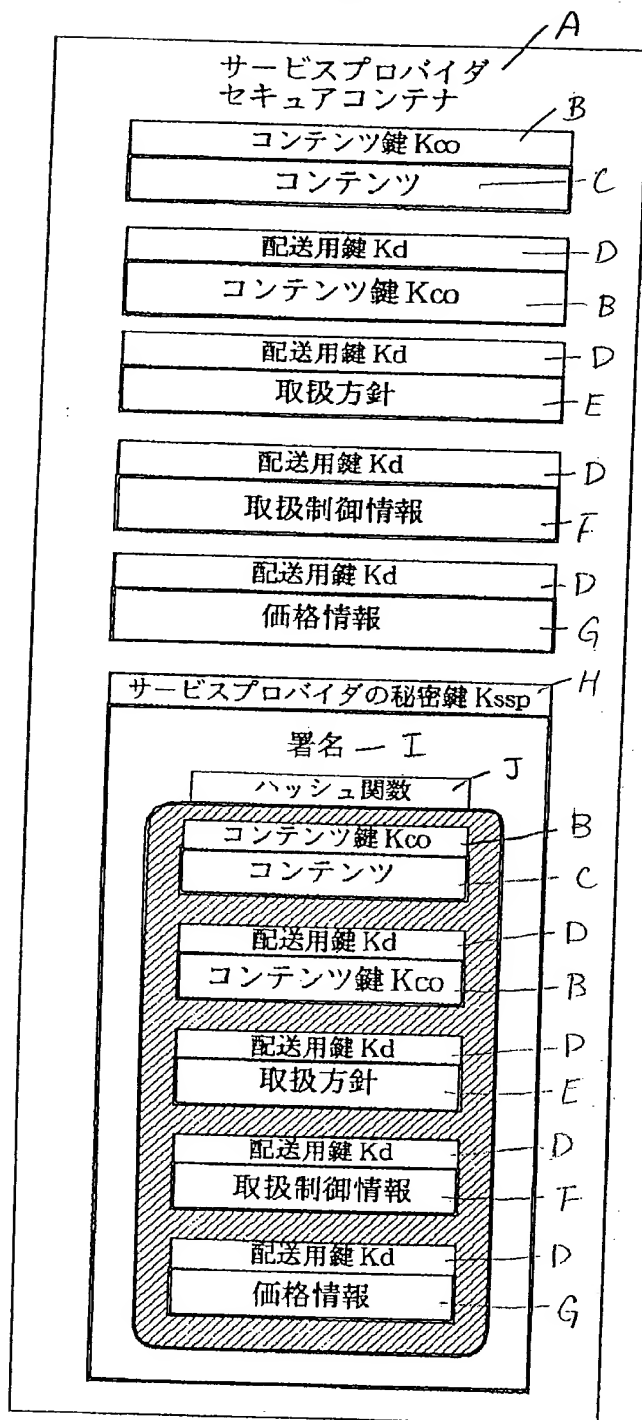
【図 22】



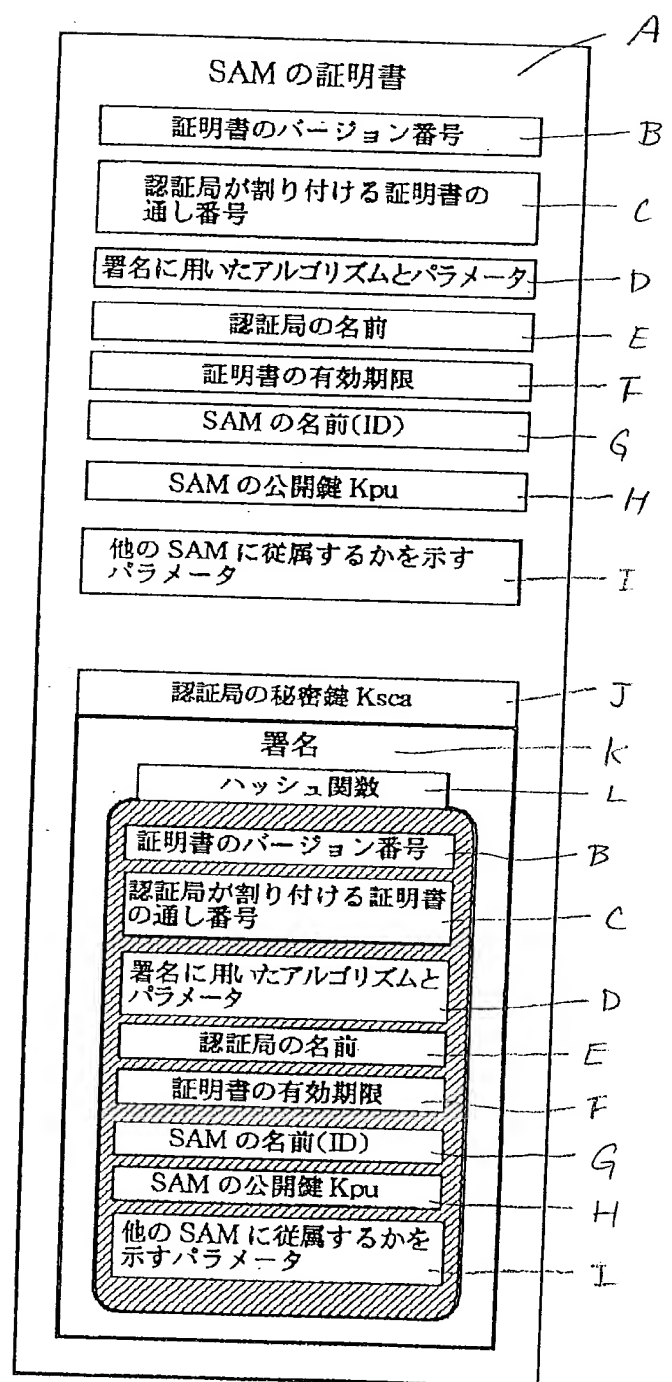
【図 25】



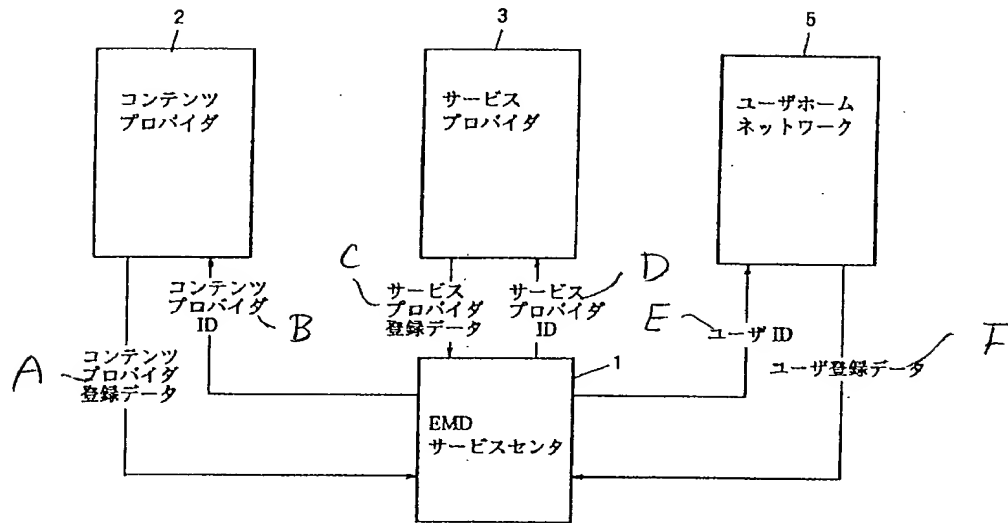
【図 26】



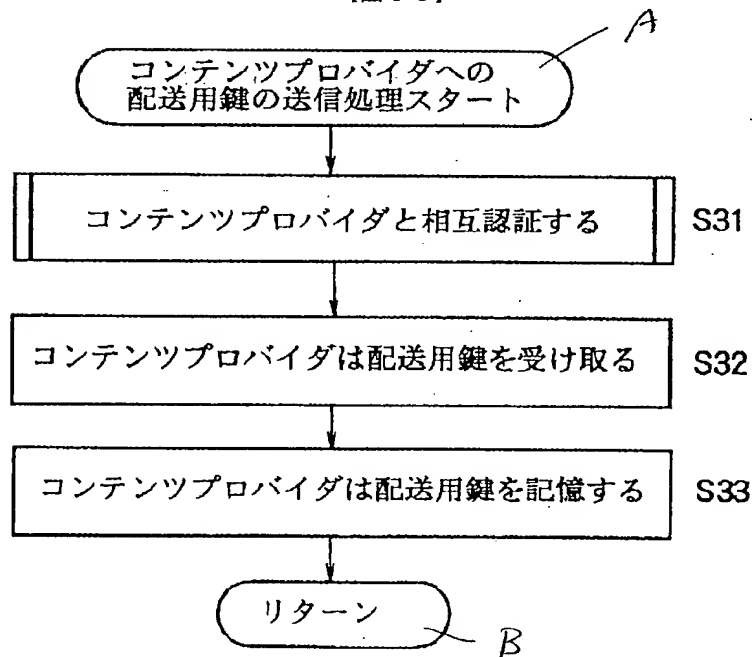
【図 41】



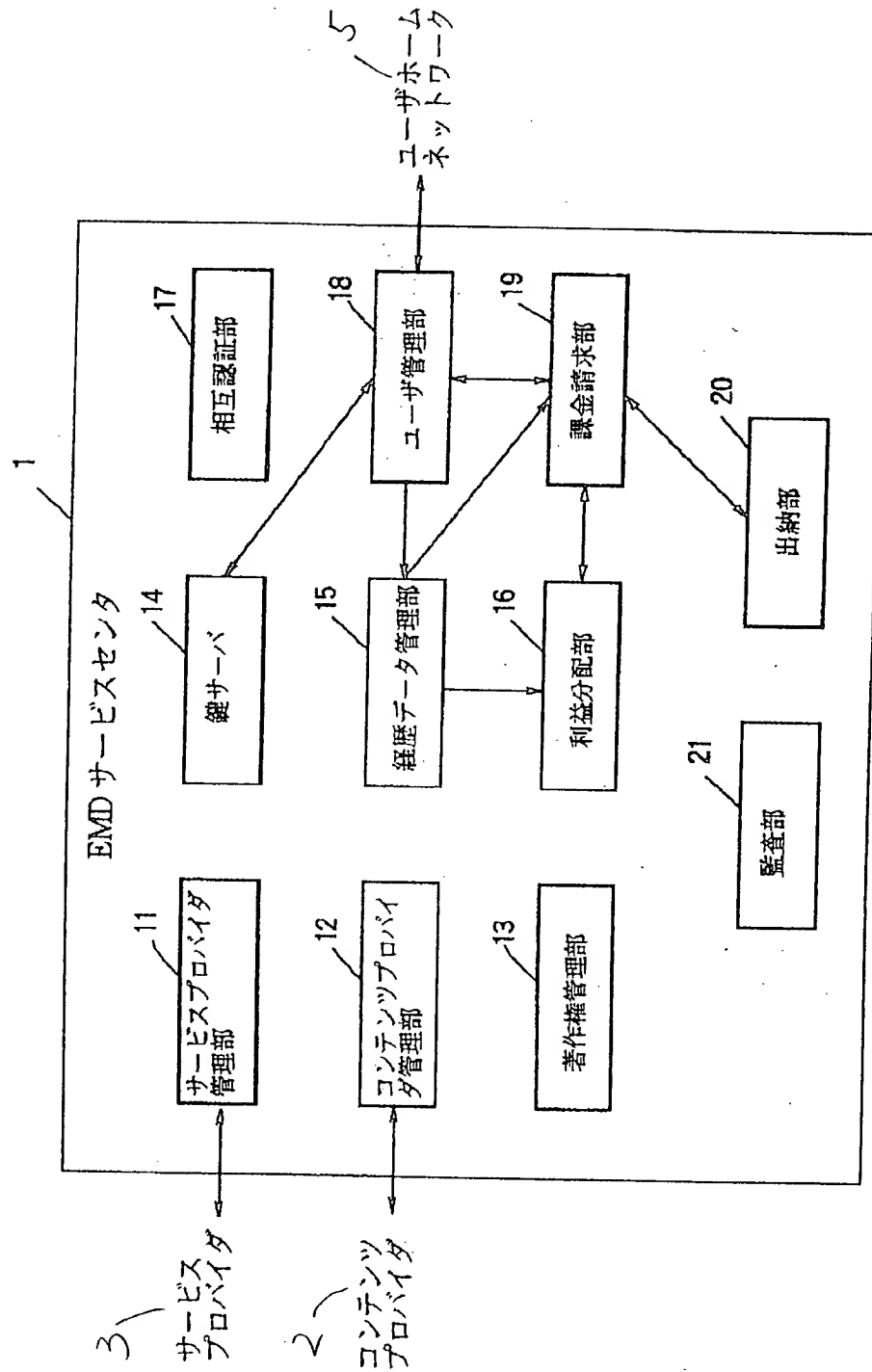
【図27】



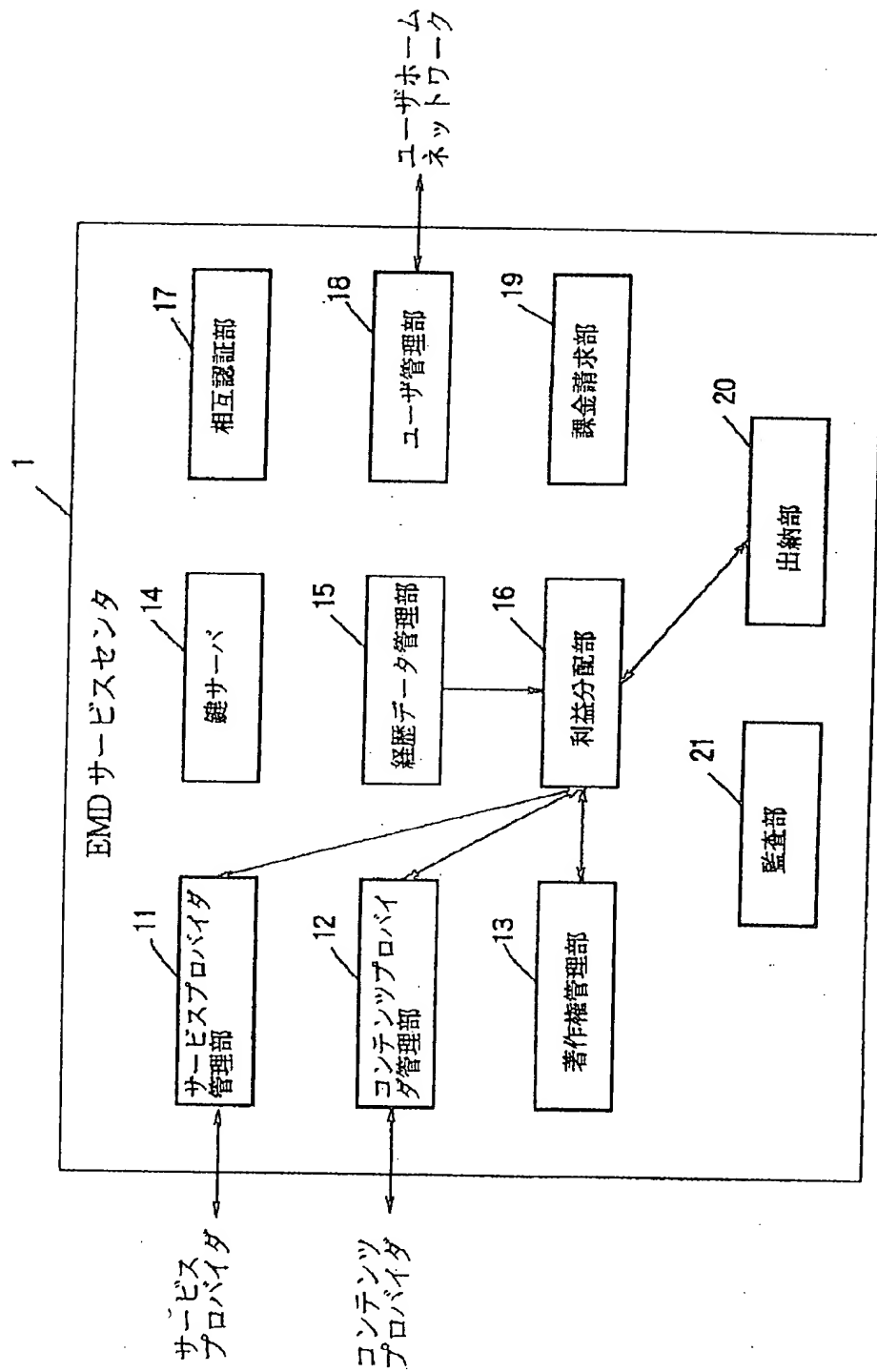
【図36】



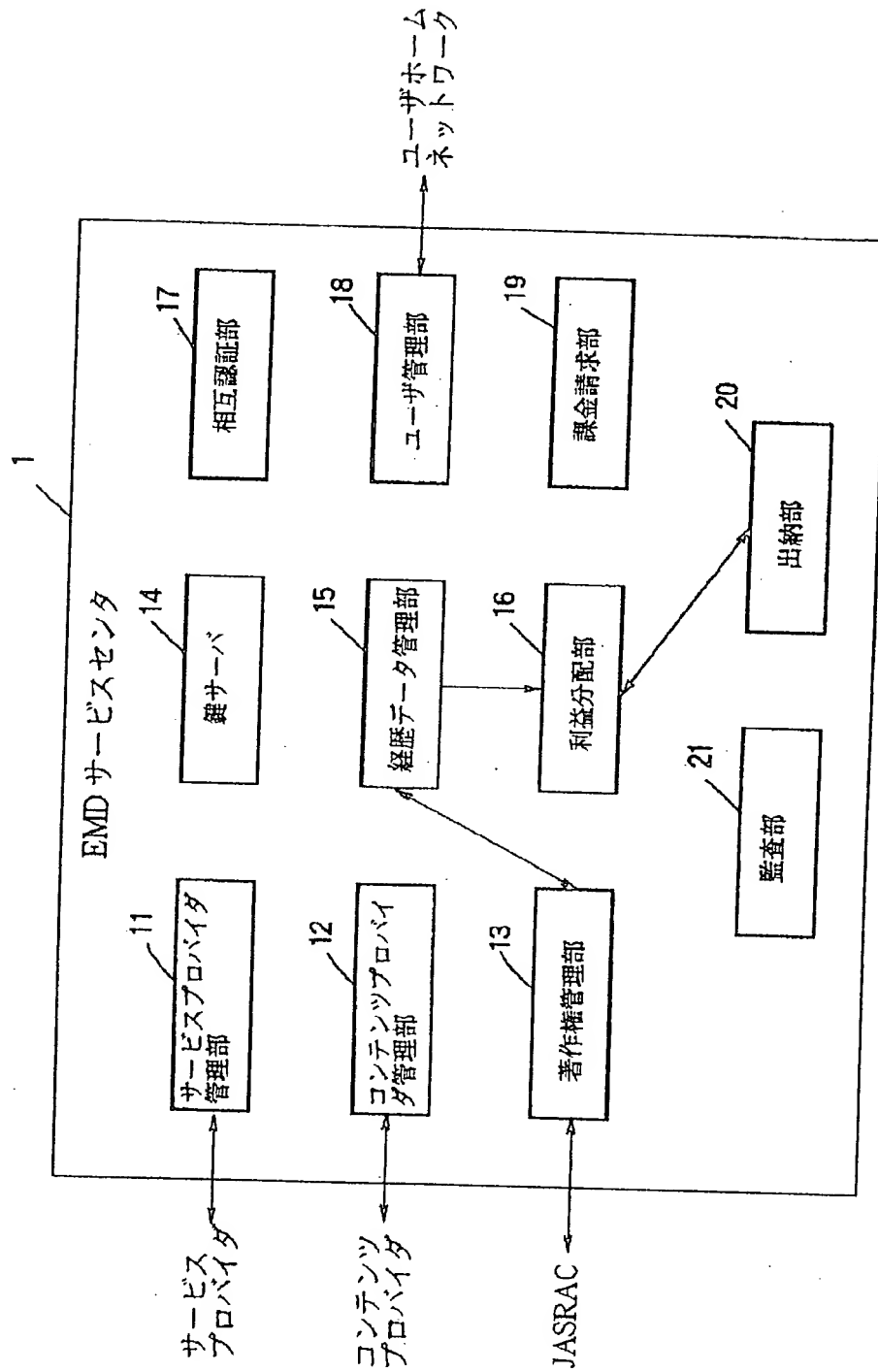
【図 31】



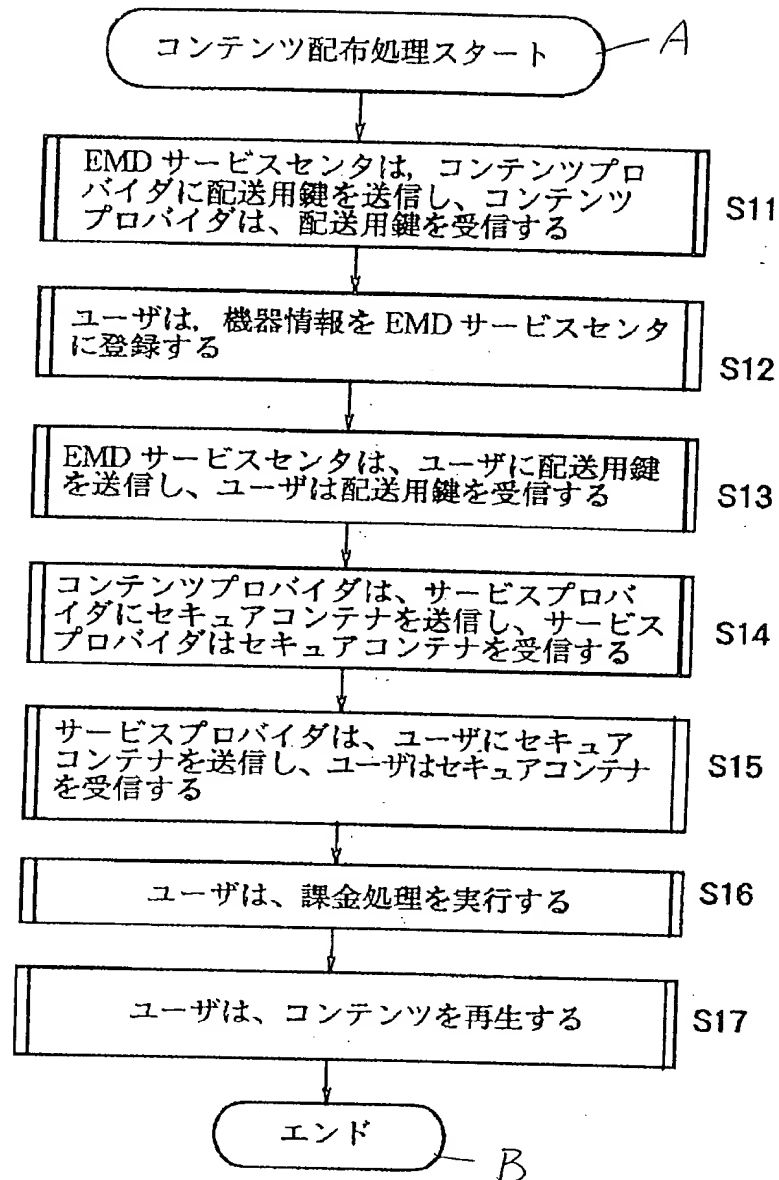
【図32】



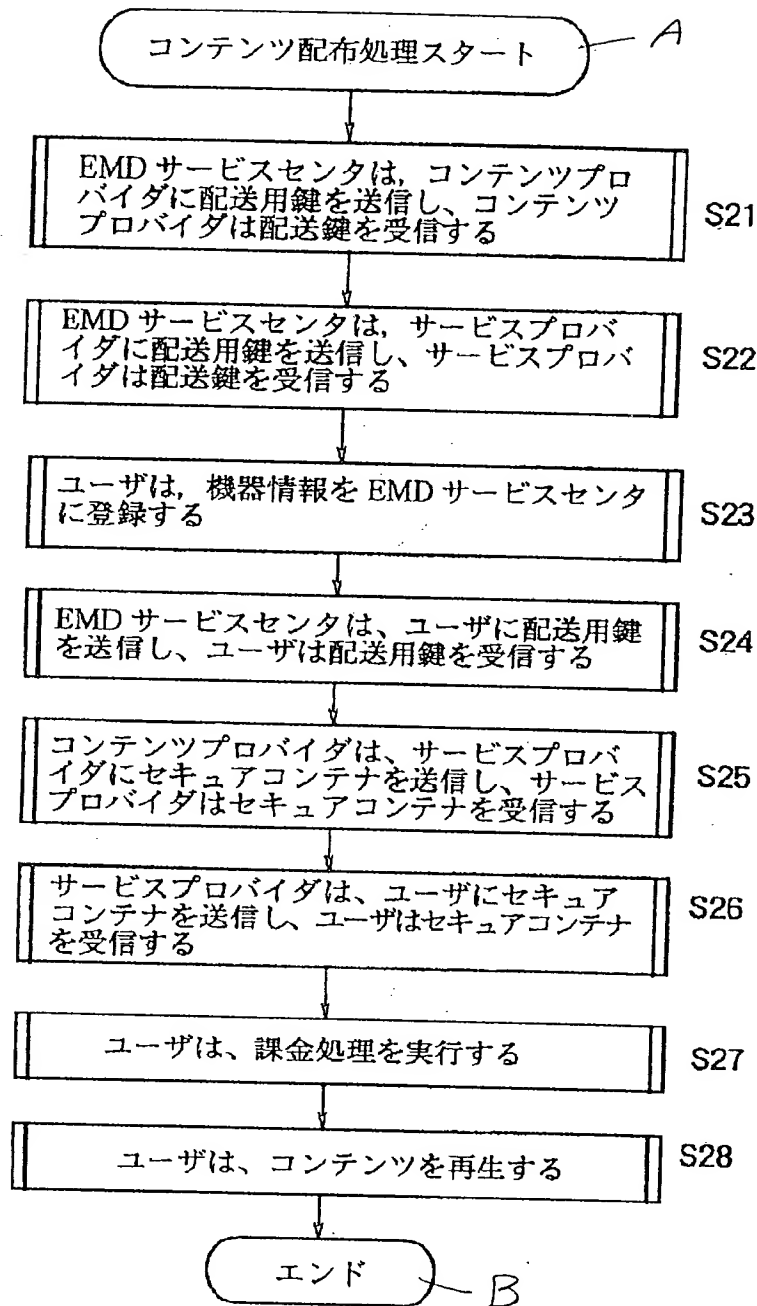
【図 33】



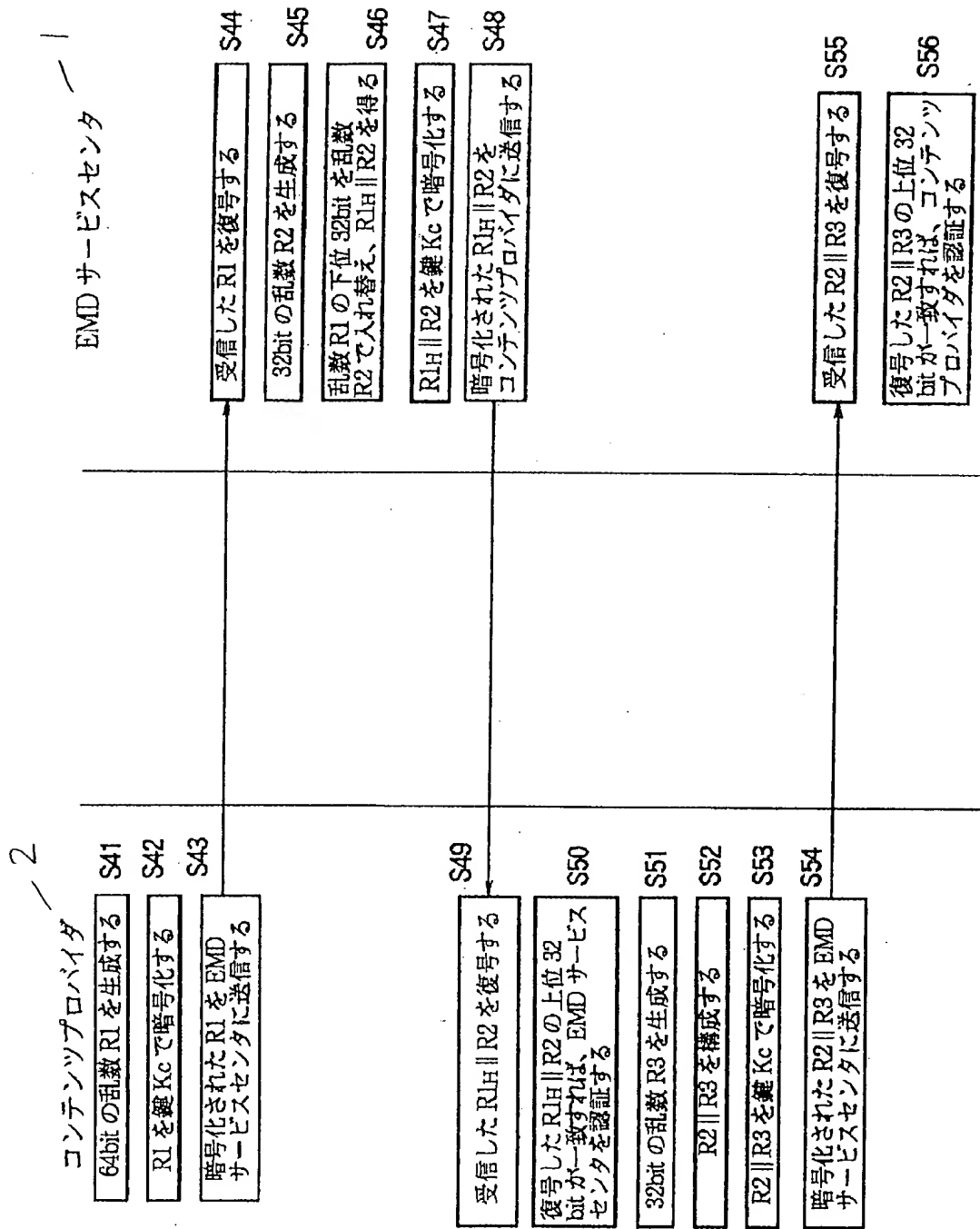
【図 34】



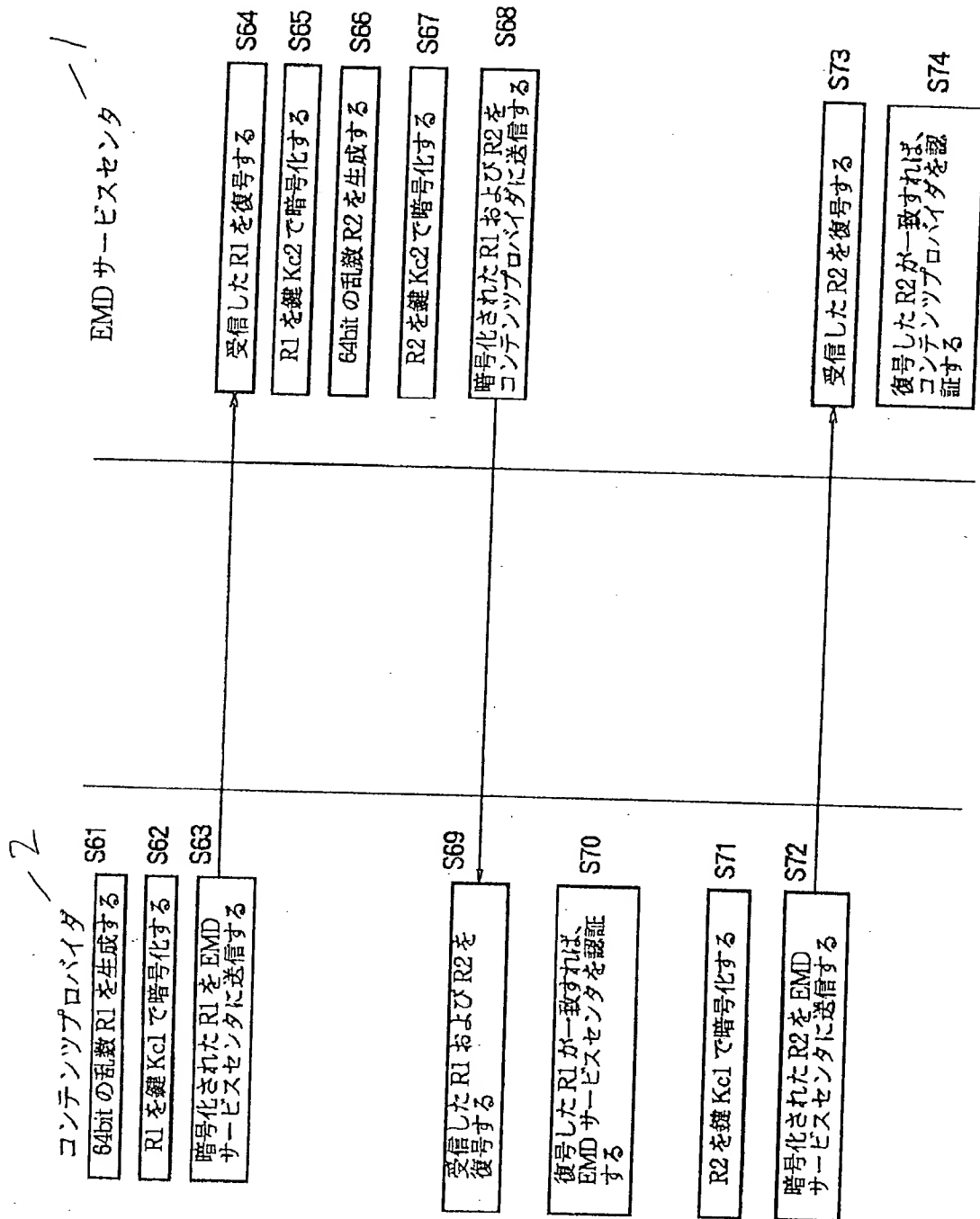
【図35】



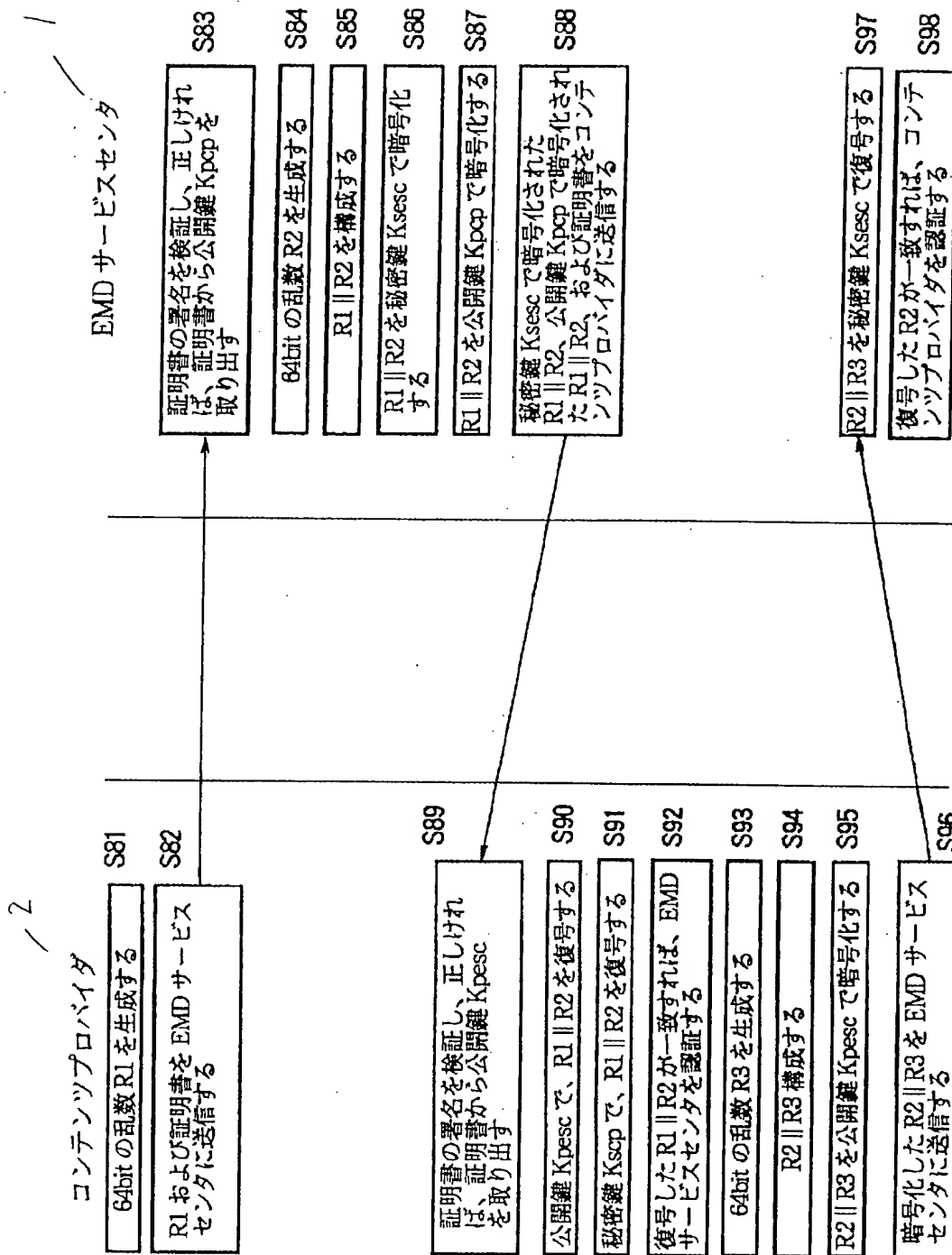
【図 37】



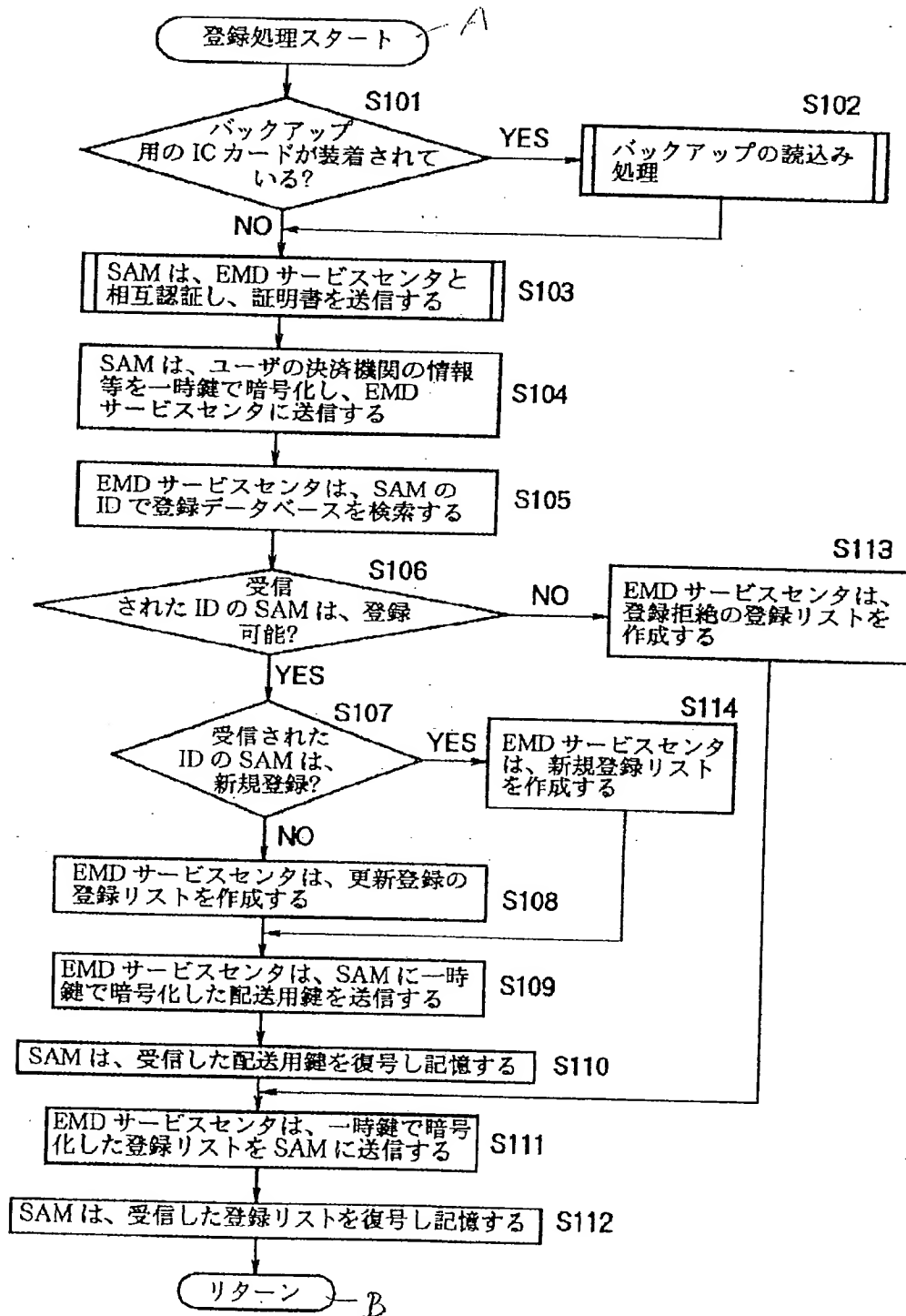
〔図 38〕



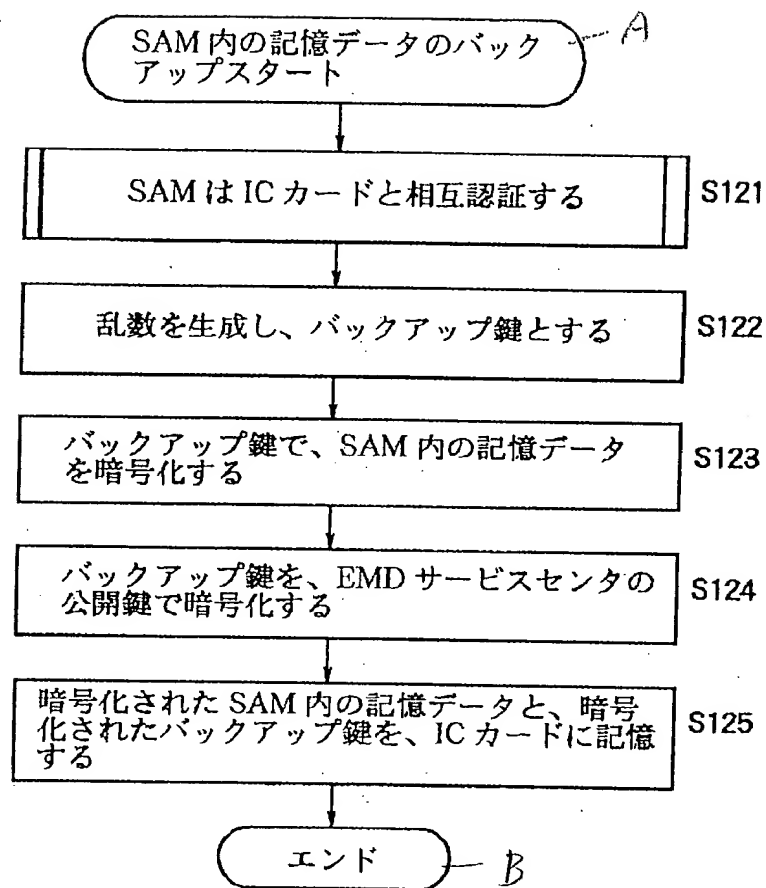
【図 39】



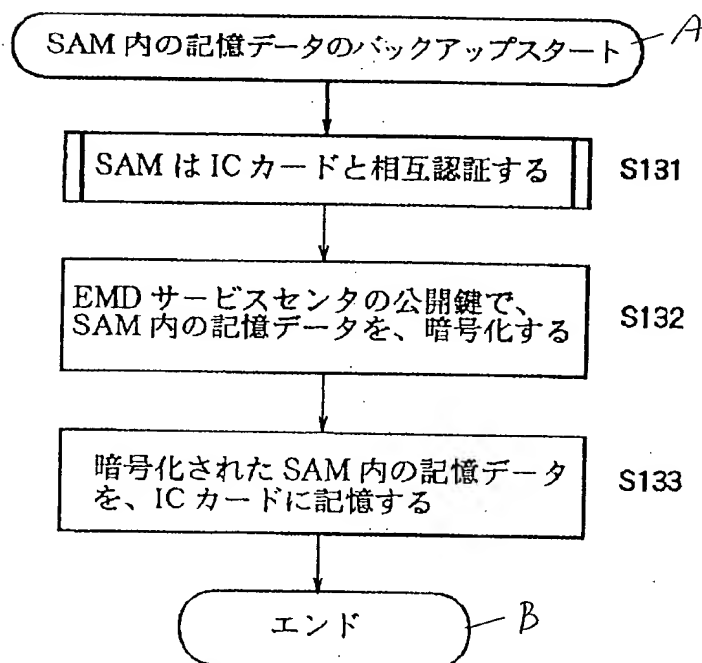
【図 40】



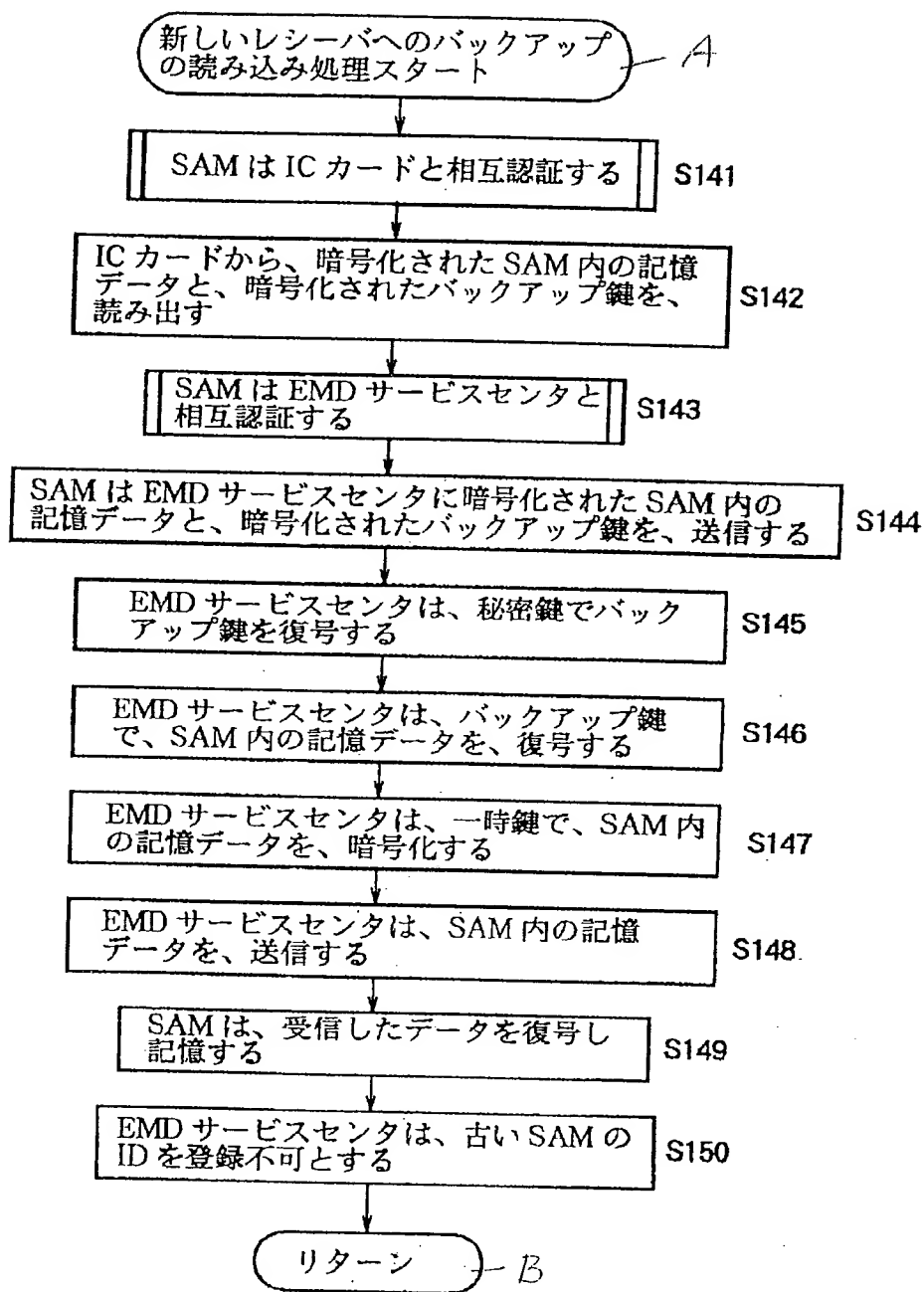
【図 4 3】



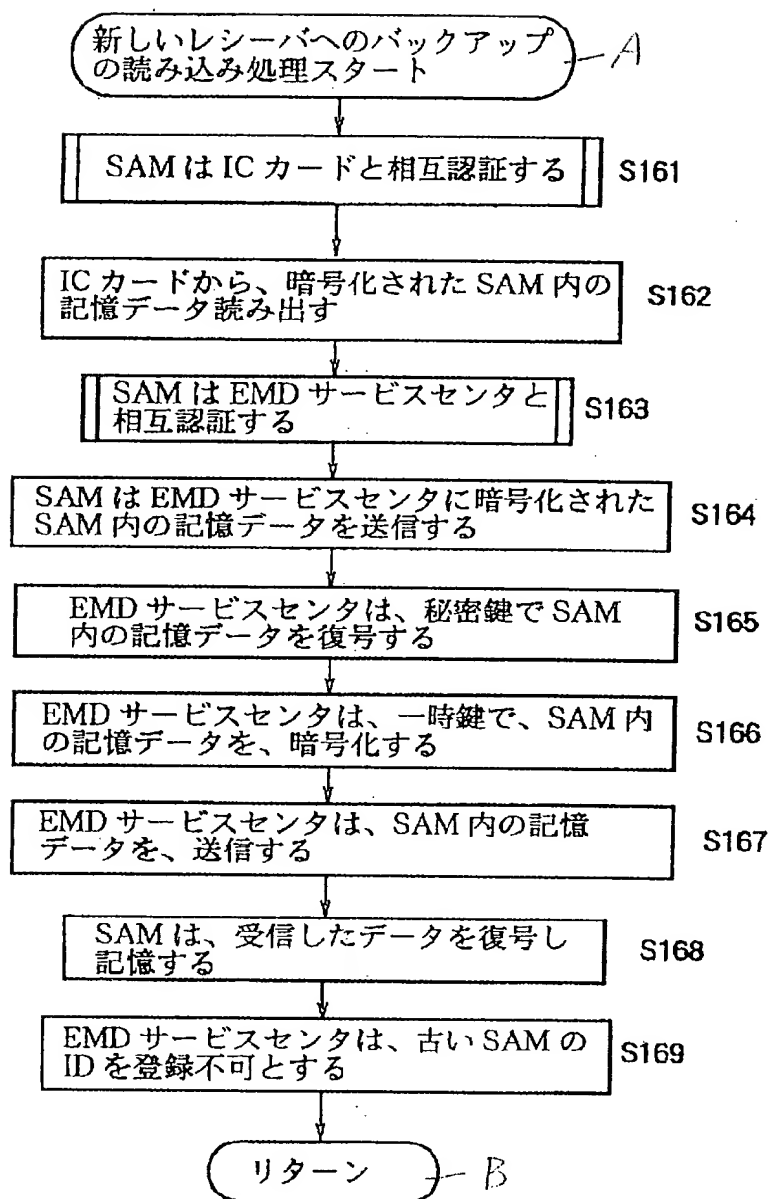
【図 4 4】



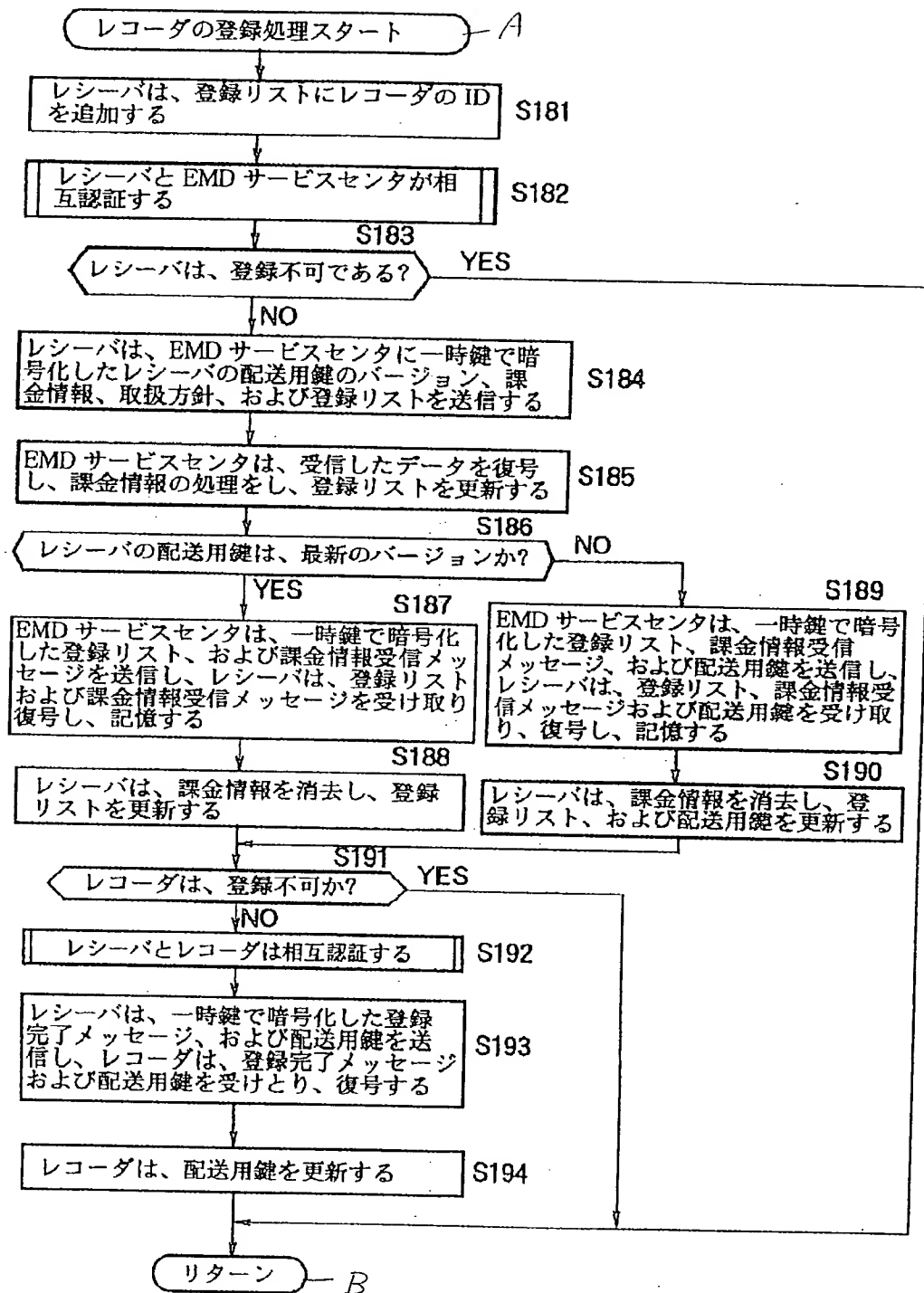
【図45】



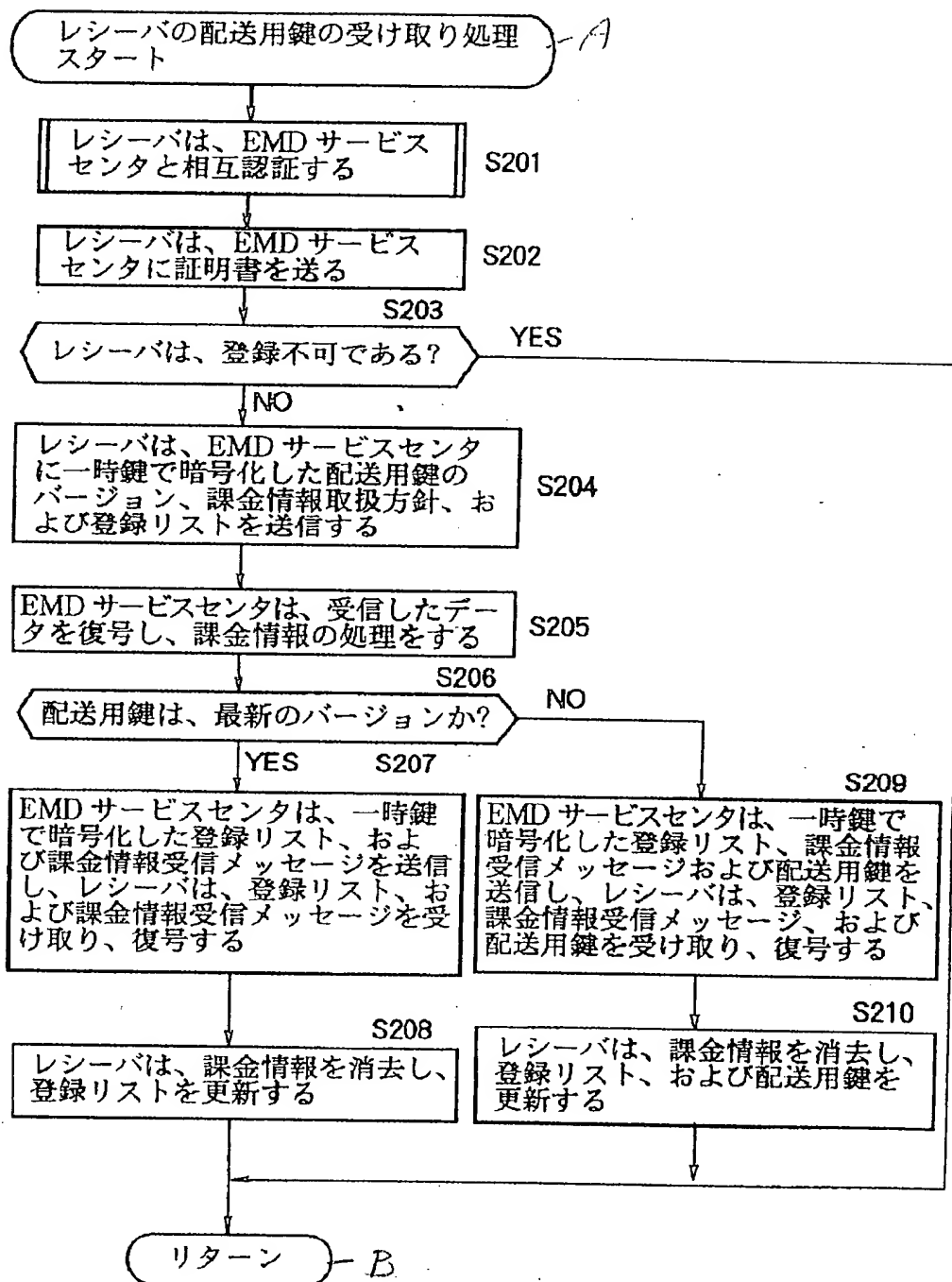
【図 46】



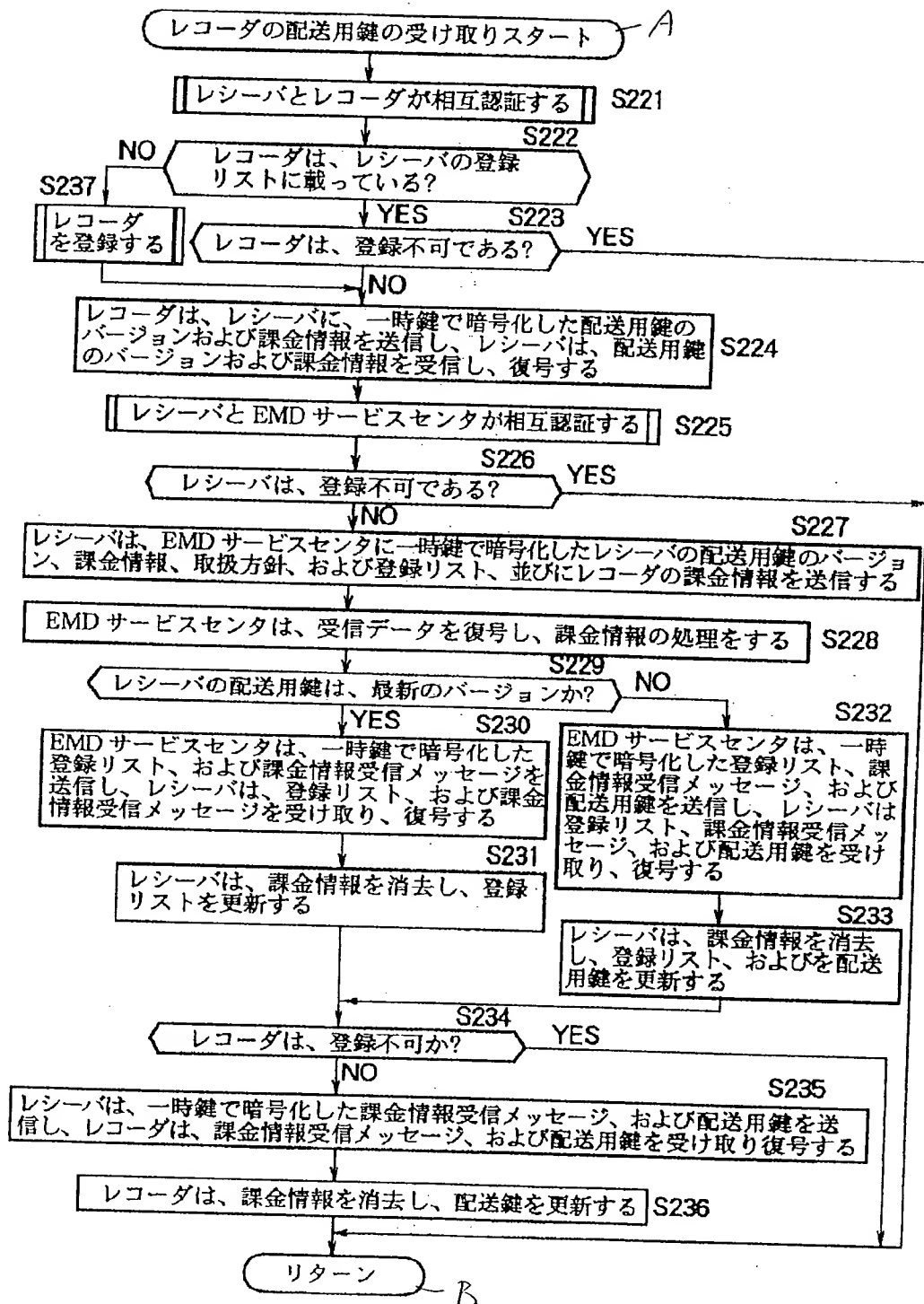
【図 47】



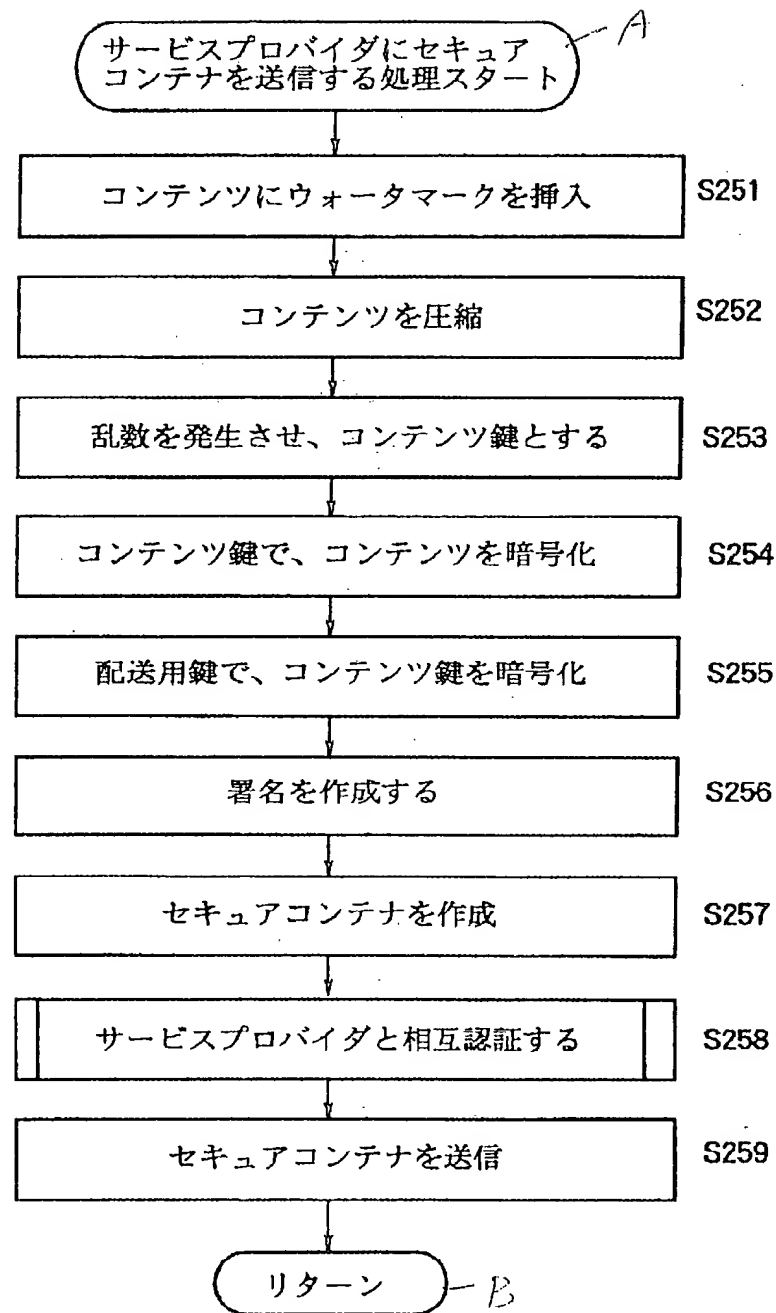
【図 48】



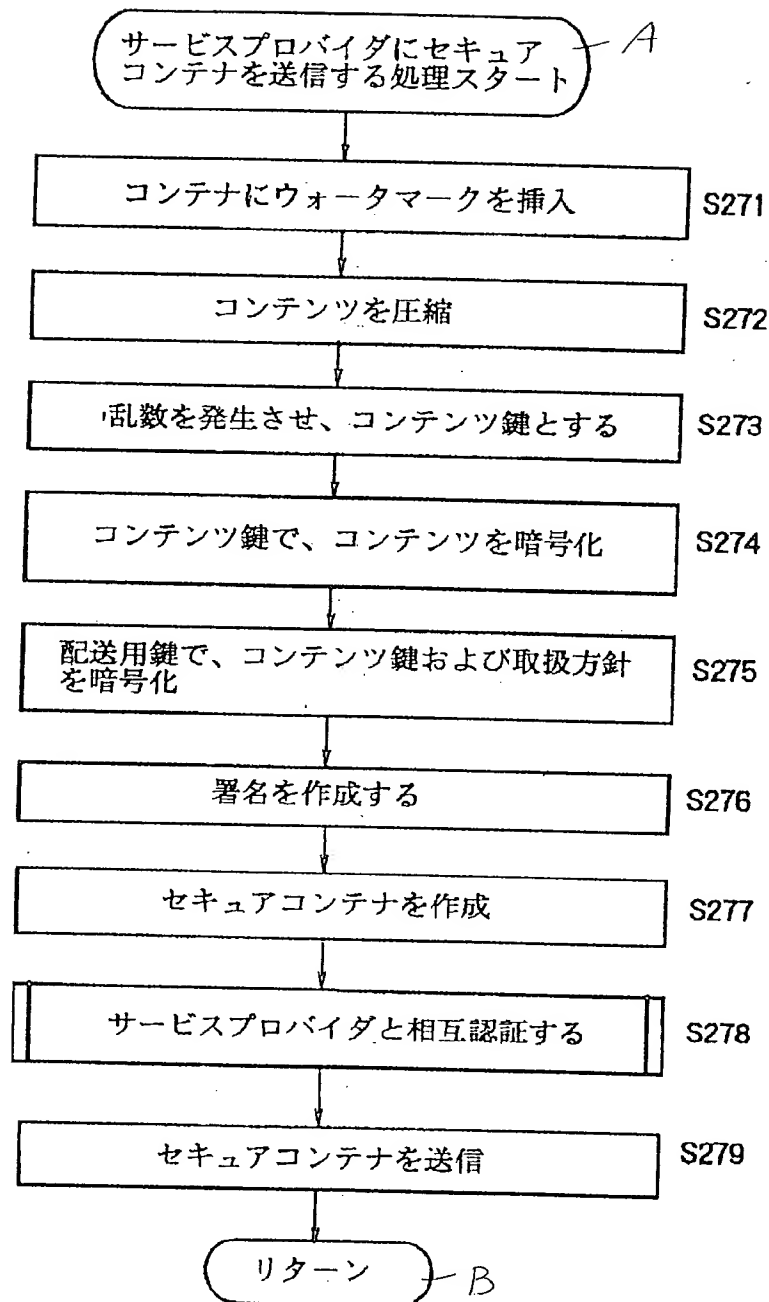
【図 49】



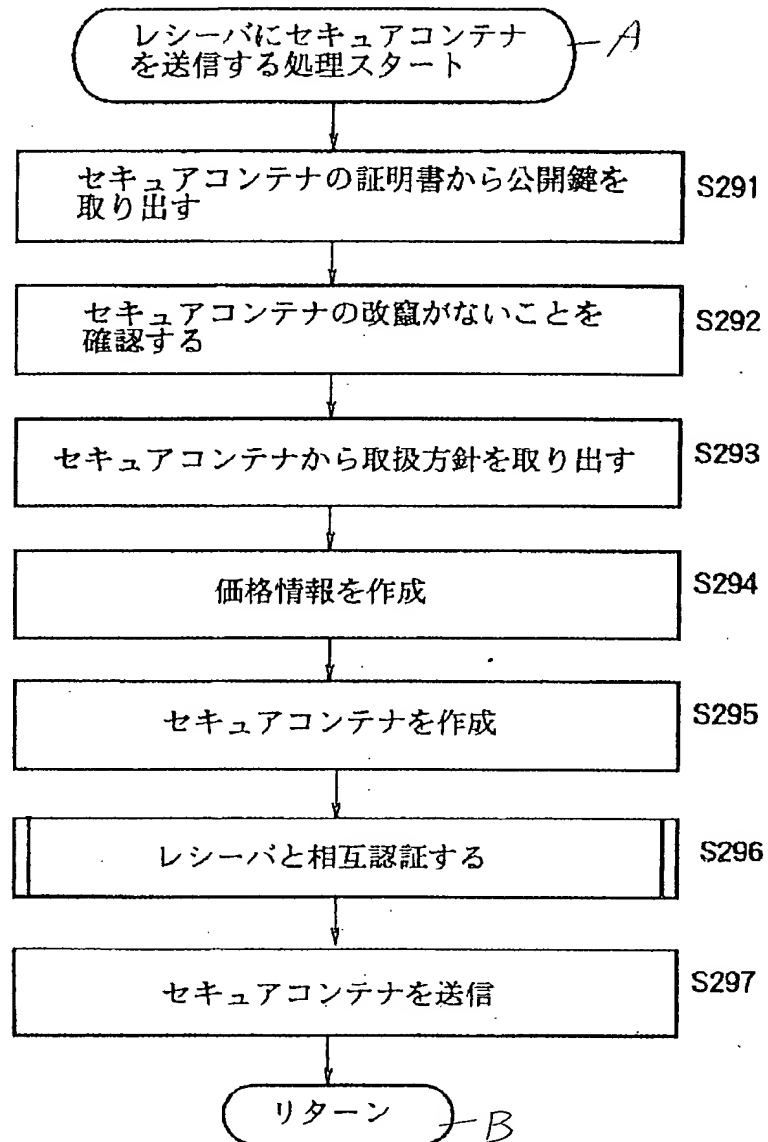
【図 50】



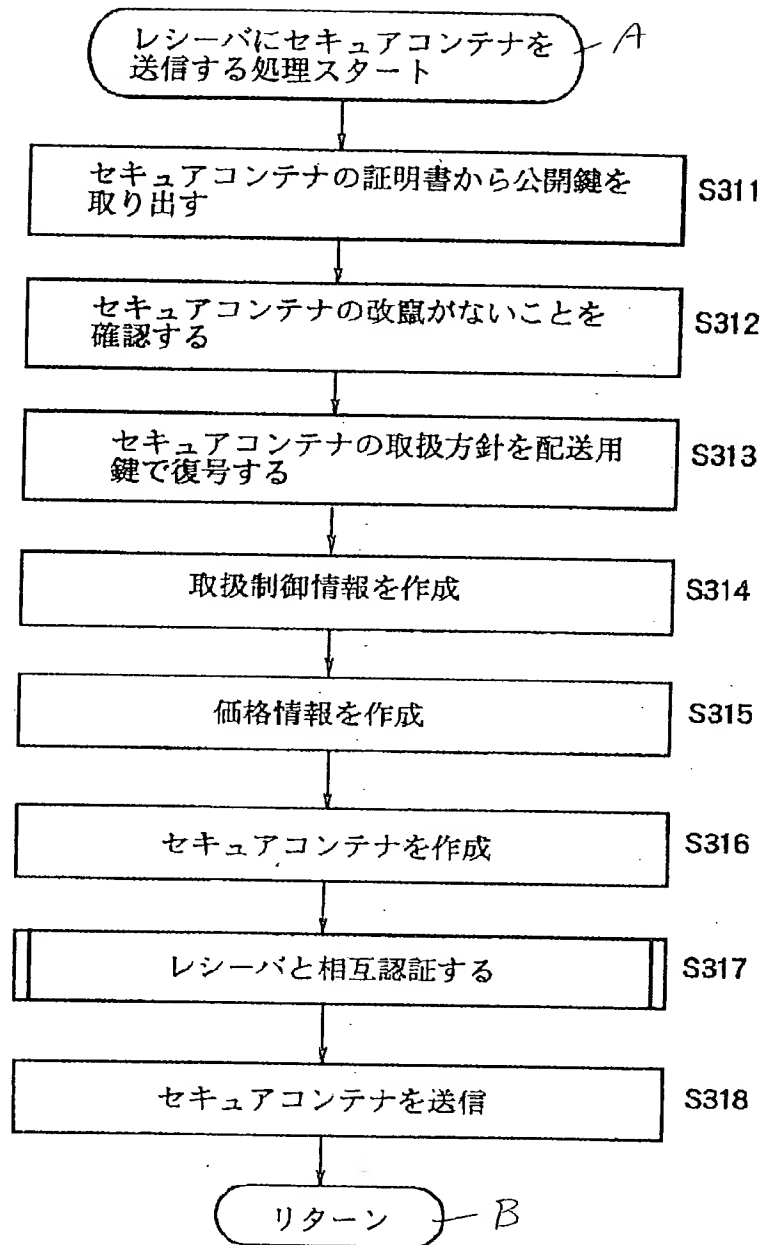
【図 51】



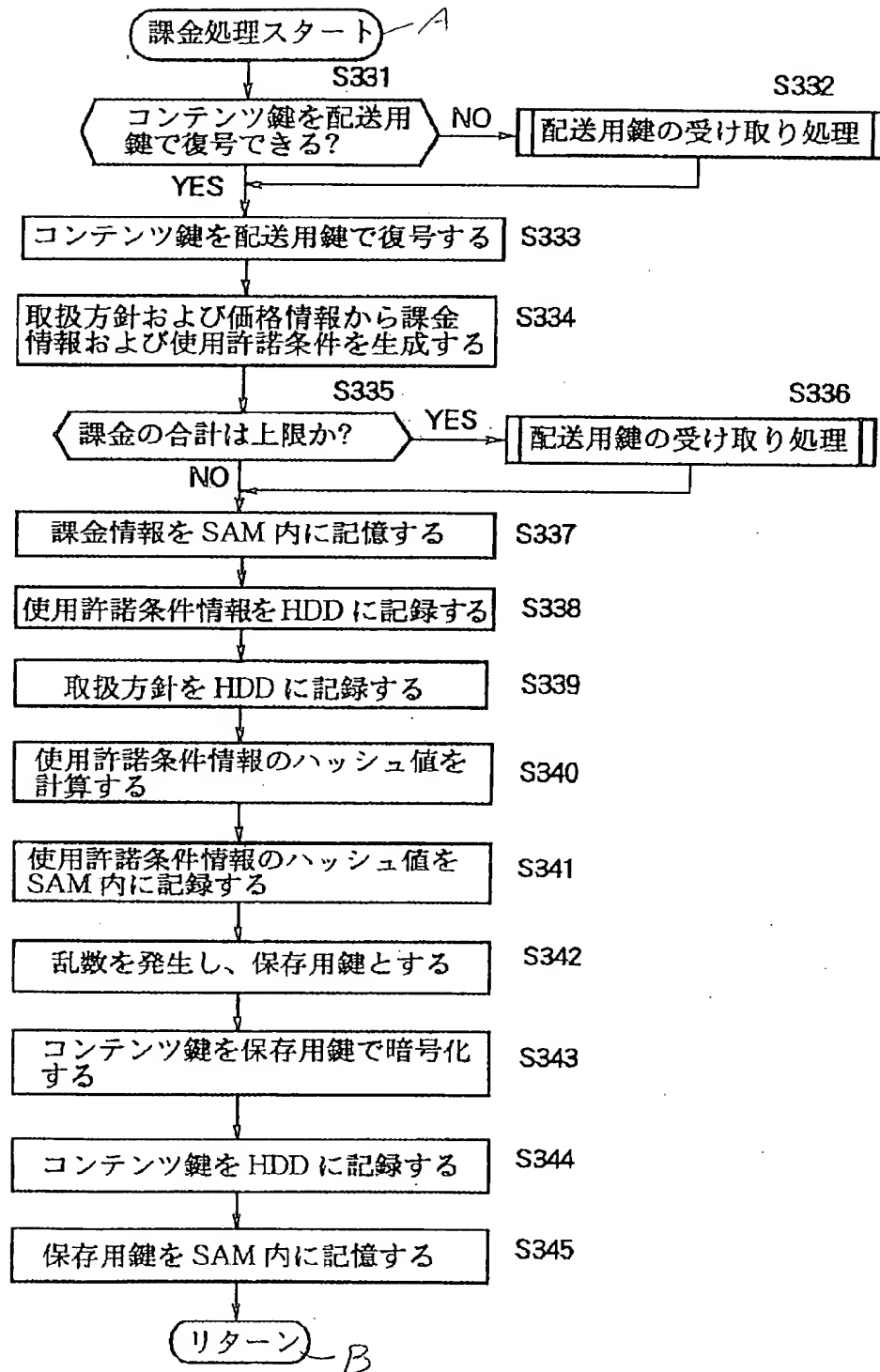
【図 52】



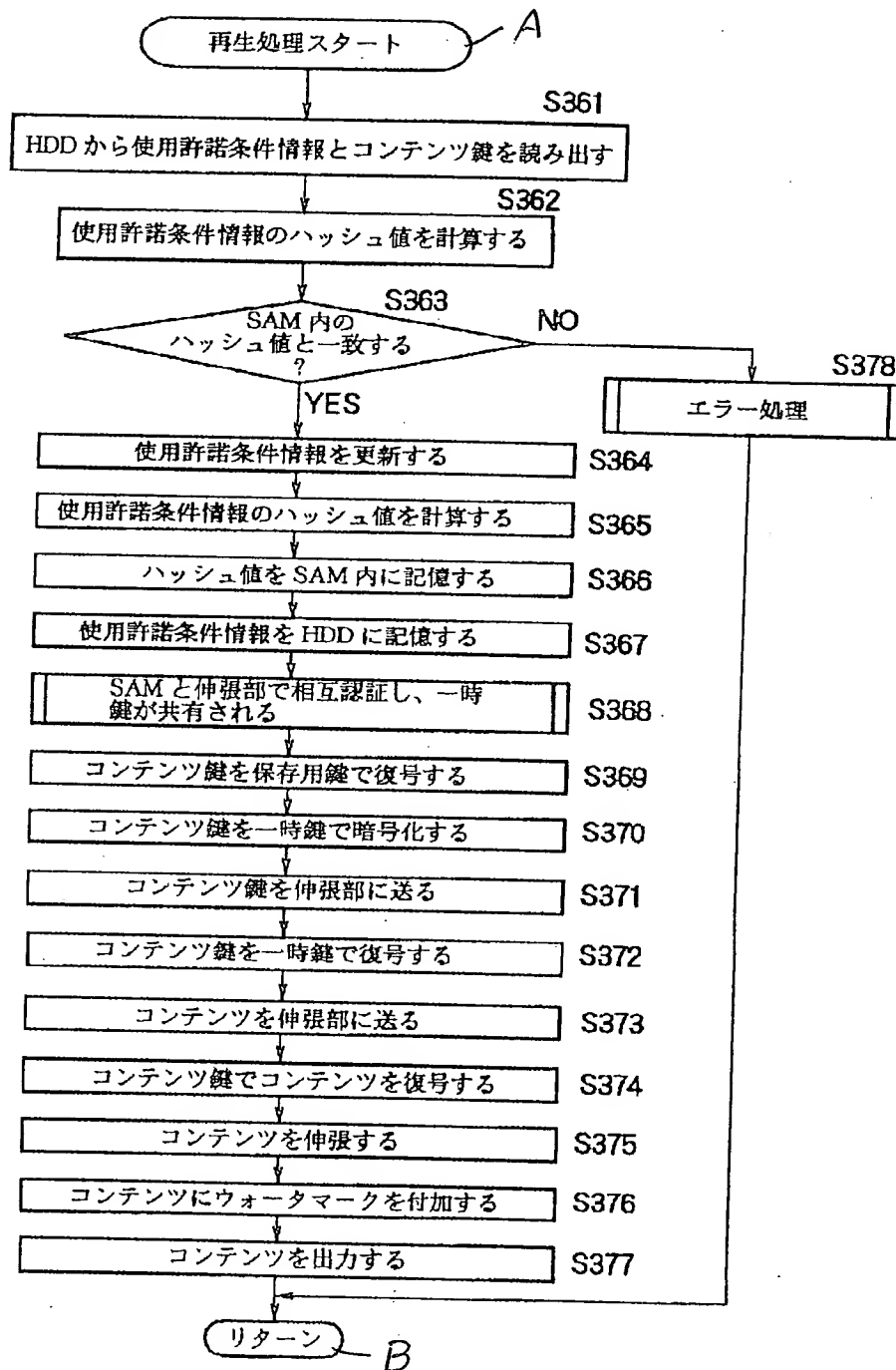
【図 53】



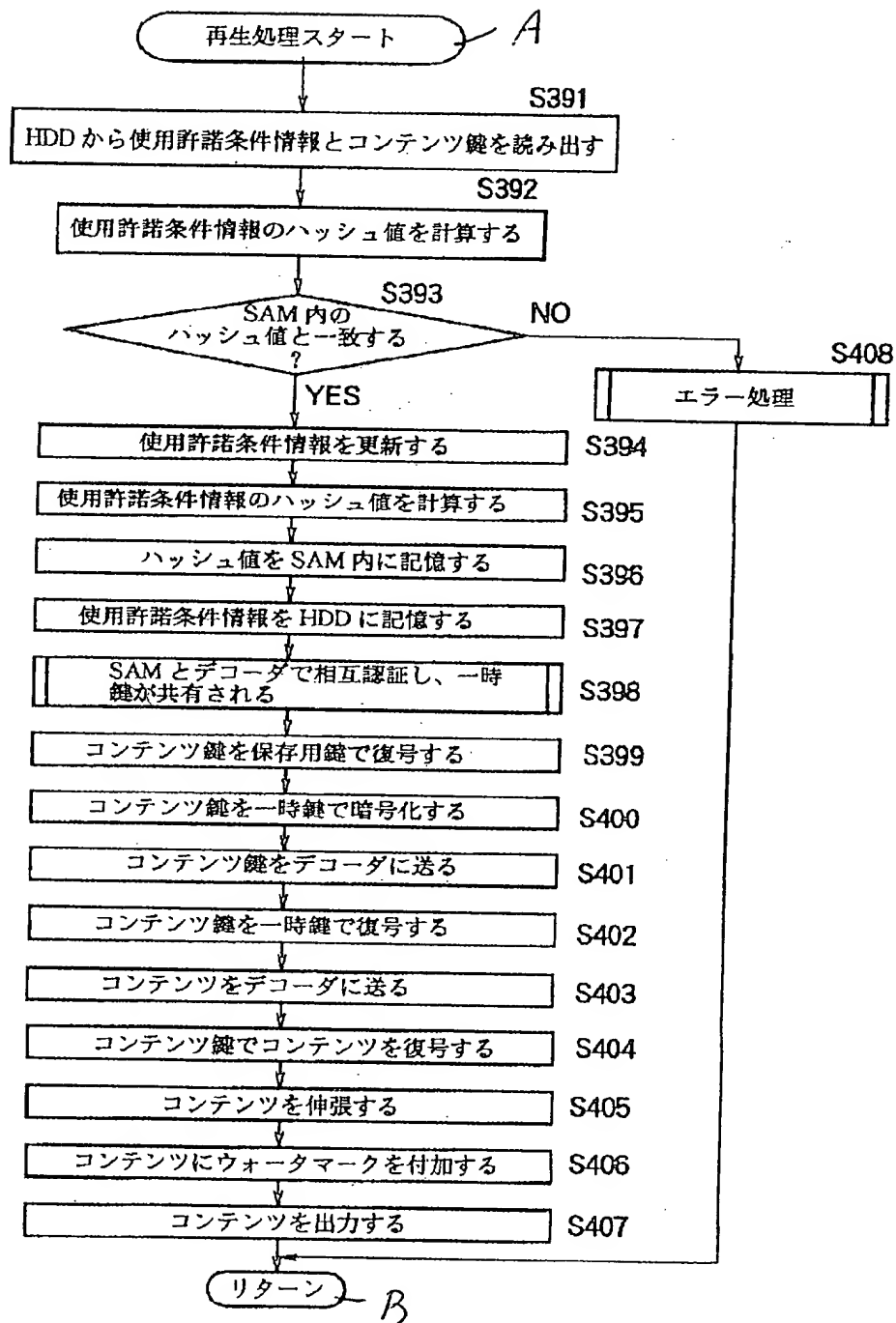
【図 54】



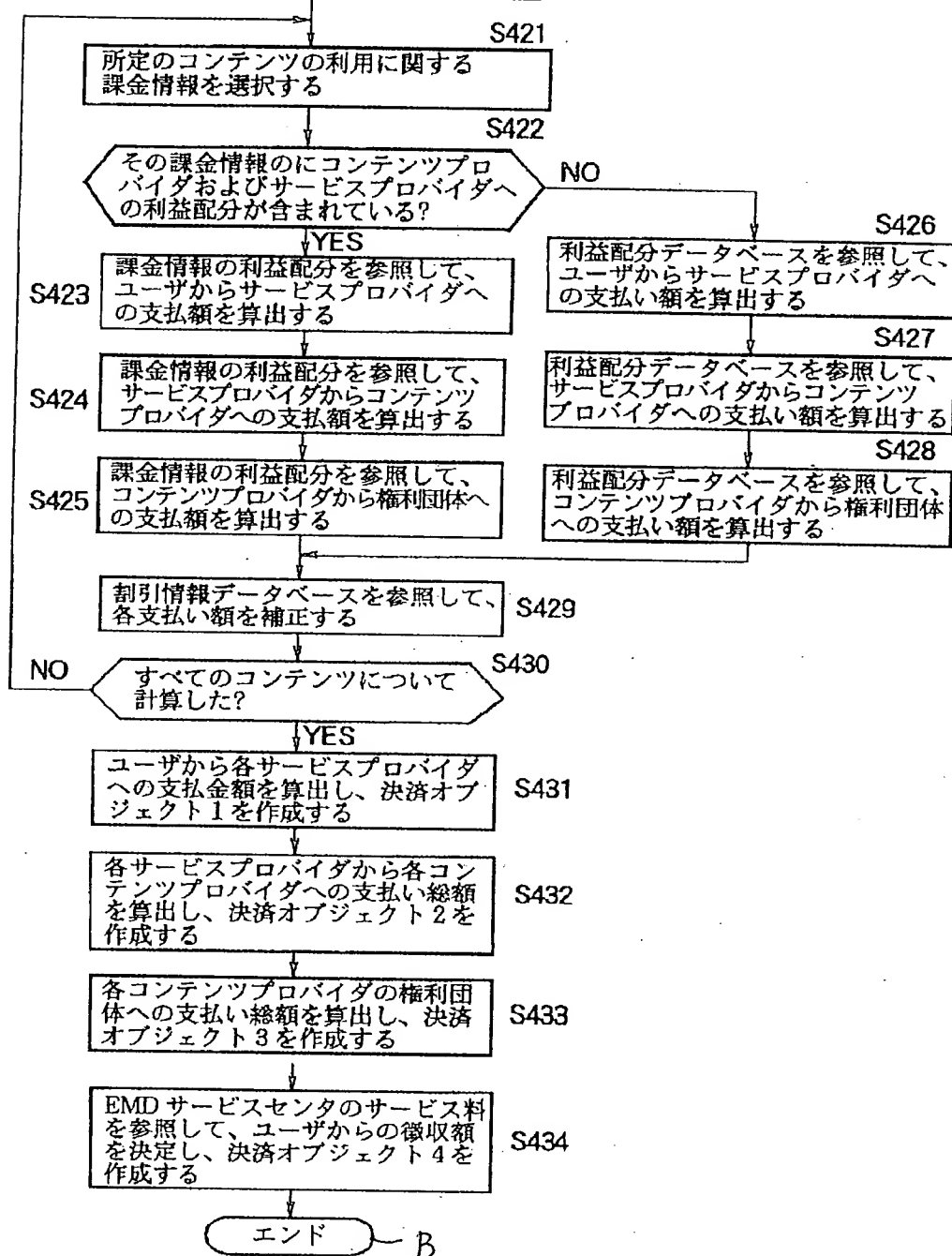
【図55】



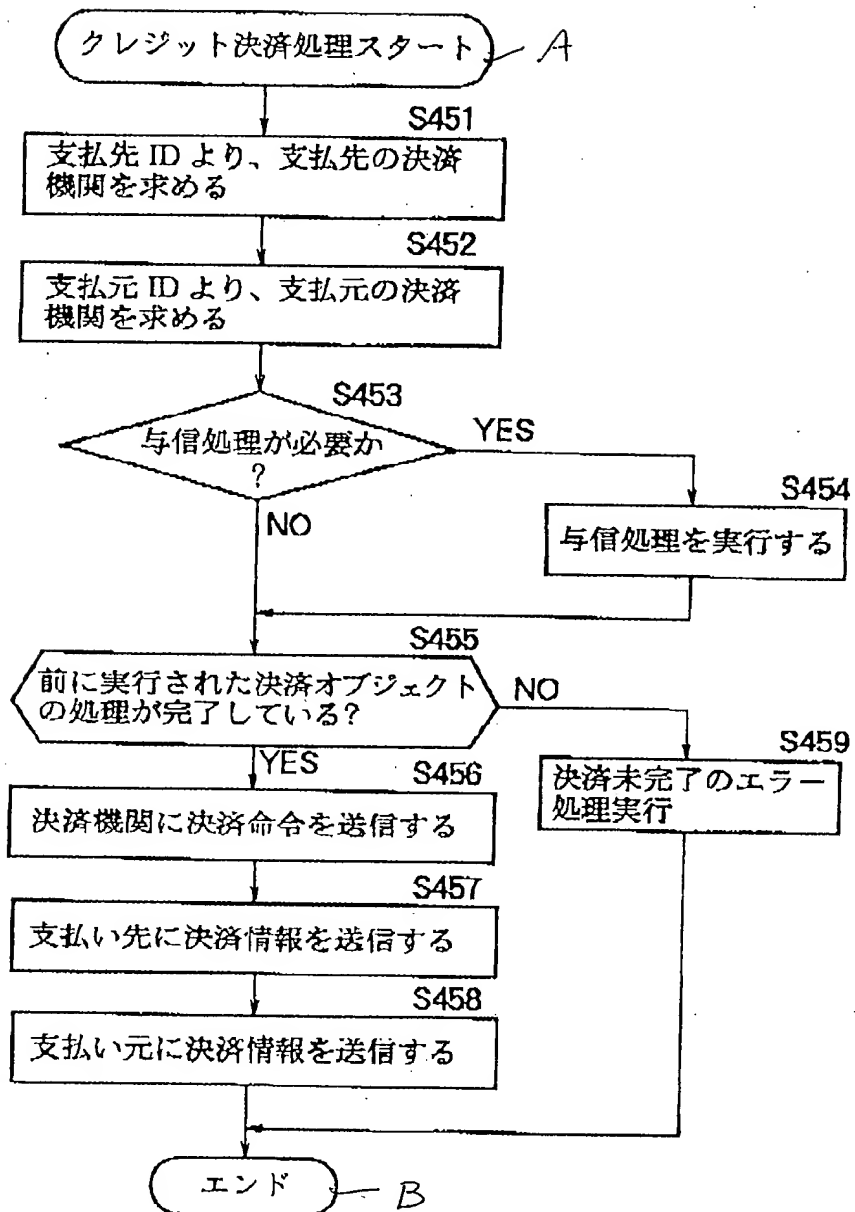
【図 56】



決済オブジェクト作成処理スタート



【図 61】



THIS PAGE BLANK (USPTO)